NOVIEMBRE 2008

INVESTIGACION Y CIENCIA

Edición española de SCIENTIFIC AMERICAN



CRIPTOGRAFIA Técnicas para guardar secretos

MEDICINA Historias clínicas confidenciales

INTERNET Escuchas en la Red

ESPIONAJE Nuevos instrumentos para la vigilancia

www.investigacionyciencia.es

6,00 EUROS

NUMERO MONOGRAFICO

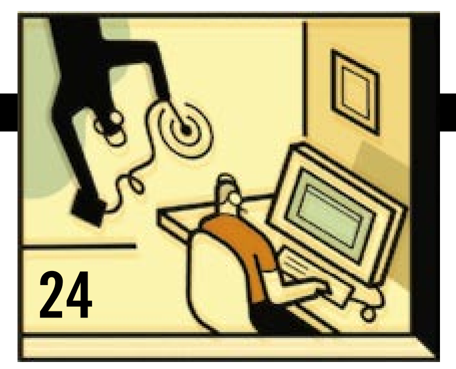
PRIVACIDAD

¿Podemos proteger nuestra intimidad personal en un mundo cada vez más intervenido?



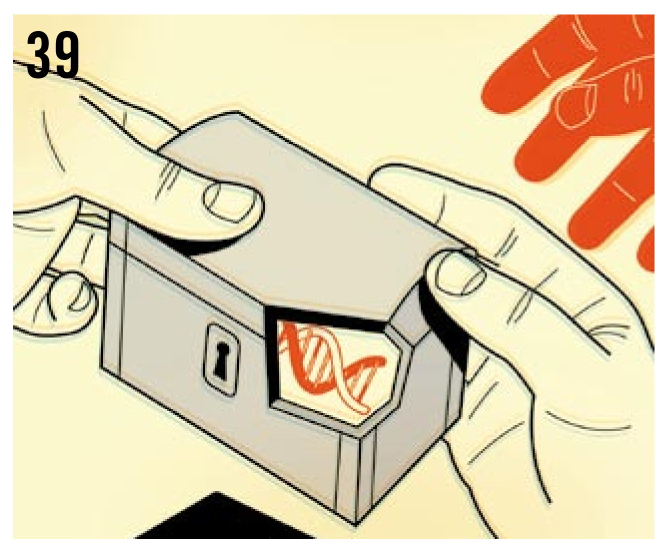
SUMARIO

Noviembre de 2008/ Número 386





También la telefonía por Internet es vulnerable a las escuchas.

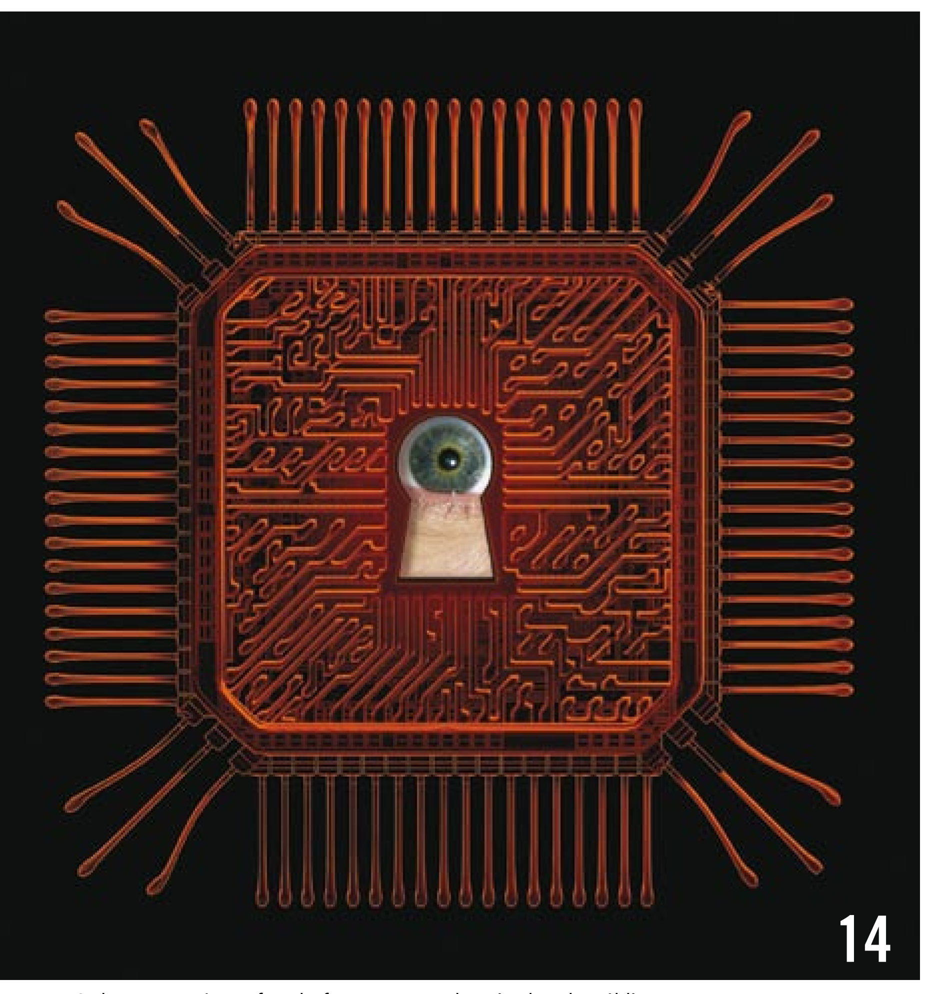


¿Deberán ser confidenciales los resultados de nuestros análisis genéticos?



Hasta con insectos mecánicos se puede espiar.

ARTICULOS



Cada vez es más confusa la frontera entre lo privado y lo público.



Las etiquetas de RFID podrían utilizarse para controlar a los ciudadanos.



Nuevas formas de cifrado protegen lo que debe permanecer secreto.

SECCIONES

INVESTIGACION Y CIENCIA

DIRECTOR GENERAL José M.ª Valderas Gallardo
DIRECTORA FINANCIERA Pilar Bronchal Garfella
EDICIONES Juan Pedro Campos Gómez
Laia Torres Casas
PRODUCCIÓN M.ª Cruz Iglesias Capón
Albert Marín Garau
SECRETARÍA Purificación Mayoral Martínez
ADMINISTRACIÓN Victoria Andrés Laiglesia
SUSCRIPCIONES Concepción Orenes Delgado
Olga Blanco Romero
EDITA Prensa Científica, S.A. Muntaner, 339 pral. 1.ª
08021 Barcelona (España)
Teléfono 934 143 344 Fax 934 145 413
www.investigacionyciencia.es

SCIENTIFIC AMERICAN

EDITOR IN CHIEF John Rennie
EXECUTIVE EDITOR Mariette DiChristina
MANAGING EDITOR Ricki L. Rusting
CHIEF NEWS EDITOR Philip M. Yam
SENIOR WRITER Gary Stix
EDITORS Steven Ashley, Peter Brown, Graham P. Collins, Mark Fischetti, Steve Mirsky, George Musser, Christine Soares y Kate Wong
CONTRIBUTING EDITORS W. Wayt Gibbs, Marguerite Holloway, Michelle Press, Michael Shermer, Sarah Simpson
MANAGING EDITOR, ONLINE Ivan Oransky
ART DIRECTOR Edward Bell
PRODUCTION EDITOR Richard Hunt

CHAIRMAN Brian Napack
PRESIDENT Steven Yee
VICE PRESIDENT Frances Newburg
VICE PRESIDENT, FINANCE, AND GENERAL MANAGER Michael Florek

DISTRIBUCION

para España:

LOGISTA, S. A.
Pol. Ind. Pinares Llanos
Electricistas, 3
28670 Villaviciosa de Odón (Madrid)
Teléfono 916 657 158

para los restantes países:

Prensa Científica, S. A.
Muntaner, 339 pral. 1.ª
08021 Barcelona

PUBLICIDAD

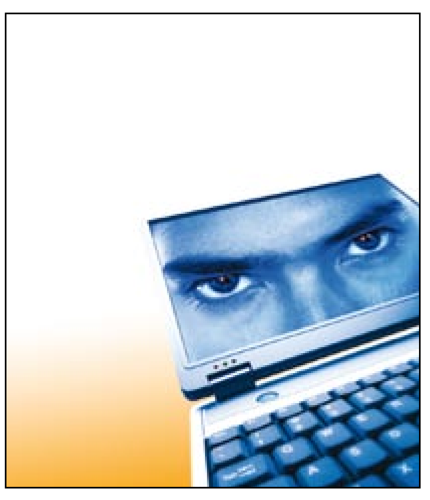
Madrid:
MMCATALAN PUBLICIDAD
M. Mercedes Catalán Rojas
Valle del silencio, 28 4.º J
28039 Madrid
Tel. 915 759 278 – Fax 918 276 474
Móvil 649 933 834

Cataluña:
Teresa Martí Marco
Muntaner, 339 pral. 1.ª
08021 Barcelona
Tel. 934 143 344
Móvil 653 340 243
publicidad@investigacionyciencia.es

COLABORADORES DE ESTE NUMERO

Asesoramiento y traducción:

Luis Bou: *El derecho a estar solo*, *Reflexiones sobre la nueva privacidad*, *Espionaje en la Red*, *Cartas*, *Puesta al día*, *Apuntes* y *Ciencia y sociedad*; M.ª Rosa Zapatero Osorio: *Ciencia y sociedad*; A. Garcimartín: *Perfiles*; Marián Beltrán: *Desarrollo sostenible*; Pilar García Villalba: *Privacidad genética*; J. Vilardell: *Más allá de la dactiloscopia*, *Protección de secretos*, *¿El fin de la privacidad?, Hace...*, *Ideas aplicadas y Curiosidades de la física*; Bruno Moreno: *Fusión de bases de datos* y *Apuntes*



Portada: Kenn Brown, *Mondolithic Studios*

SUSCRIPCIONES

Prensa Científica S. A.
Muntaner, 339 pral. 1.ª
08021 Barcelona (España)
Teléfono 934 143 344
Fax 934 145 413

Precios de suscripción:

	Un año	**Dos años**
España	65,00 euro	120,00 euro
Resto del mundo	100,00 euro	190,00 euro

Ejemplares sueltos:

El precio de los ejemplares atrasados es el mismo que el de los actuales.



ISSN 0210136X Dep. legal: B. 38.999 – 76

Imprime Rotocayfo S.L. (Impresia Ibérica) Ctra. de Caldes, km 3 - 08130 Santa Perpètua de Mogoda (Barcelona)

Printed in Spain - Impreso en España



¿Reciclado peligroso?

En "El reciclado nuclear" (Investigación y Ciencia, julio de 2008), Frank N. von Hippel explica por qué quiere la desaparición del reciclado nuclear. Pero no va a desaparecer. La energía nuclear está resurgiendo, tanto en los EE.UU. como en otras partes del mundo. Seguir desechando como "residuo" el 99 por ciento de la energía existente en la mena de uranio resulta claramente insostenible.

El procesamiento se está difundiendo inexorablemente, con el consiguiente aumento de la posibilidad de un uso perverso para la producción de armas. Para minimizar tal riesgo, el procesamiento de combustible ha de realizarse bajo auspicios internacionales, con garantías absolutas de que los países tendrán acceso ininterrumpido al combustible si abandonan sus propias instalaciones de enriquecimiento y reciclado.

Von Hippel afirma correctamente que el uso de MOX (mezcla de óxidos de plutonio y uranio) para reciclar el plutonio y reutilizarlo en los reactores "térmicos" de nuestros días resulta oneroso, que su utilidad es muy escasa y que produce plutonio cuyo grado de pureza química lo hace apto para armamentos. Pero los métodos de reciclado para reactores avanzados de neutrones rápidos son diferentes. Tales métodos se orientan a la utilización de recursos, y no olvidan los problemas de los residuos y de la proliferación nuclear [*véase* "Residuos nucleares", en Investigación y Ciencia, febrero de 2006].

La técnica puede, por sí sola, suprimir la amenaza de la proliferación. La Asociación Global de la Energía Nuclear constituye un paso útil hacia una gestión prudente, y ha sido suscrita hasta ahora por unos 21 países. Pero a falta de un continuado liderazgo de EE.UU., se quedará sin impulso y acabará por desaparecer. Se perderá la coordinación. La técnica para la producción de materiales aptos para armamentos nucleares se expandirá sin control.

William H. Hannum, Gerald E. Marsh
y **George S. Stanford**
Laboratorio Nacional de Argonne
(jubilados)

RESPONDE VON HIPPEL: *La energía nuclear puede rebajar hasta en un 15 por ciento el aumento de las emisiones de gases con efecto invernadero. Por otra parte, el reciclado se traduce en precios más elevados de la energía eléctrica nuclear y echa abajo, además, la barrera que media entre la producción de energía y las armas nucleares.*

Hannum, Marsh, Stanford y yo mismo estamos de acuerdo en que el reciclado de plutonio en reactores refrigerados por agua carece de sentido, lo mismo en el plano técnico que en el económico. Una docena de países han dejado de renovar sus contratos de reprocesado con Francia, Rusia o Reino Unido. Areva, que es la compañía francesa de reprocesado, no ha podido acordar todavía una prolongación de su contrato con las sociedades francesas de electricidad nuclear por más de un año. El Reino Unido está renunciando por completo al reciclado.

Los reactores de neutrones rápidos, refrigerados por sodio líquido, que utilizasen material reciclado sí podrían fisionar el plutonio casi por completo, pero son tan caros, que ninguna organización privada está dispuesto a invertir en ellos. Si llegasen a quedar resueltos los problemas de coste y el riesgo de proliferación, el posible recurso energético que ofrecen el plutonio y el uranio del combustible agotado todavía estaría disponible. En el ínterin, hemos de librarnos de centenares de toneladas de plutonio ya extraído, herencia de la guerra fría, y de expectativas prematuras sobre reactores nodriza. No habrá necesidad, en un futuro previsible, de extraer más.

Línea móvil

En "La génesis de los planetas", de Douglas C. Lin (Investigación y Ciencia, julio de 2008), se dice que, según la teoría hoy predominante sobre la formación de los planetas, éstos se constituyen en el seno de un disco de gas que gira en torno a una estrella. A cierta distancia de la estrella se encuentra una "línea de hielo", allende la cual el agua se mantiene en estado sólido. Me interesa la estabilidad de esta línea gélida. Parece que debería desplazarse al progresar el disco. ¿Podría ser ésta la causa de que la Tierra posea océanos?

Tom Brown
Gainesville, Florida

RESPONDE LIN: *En efecto, la línea de hielo evoluciona. Debido a la intensa irradiación y al calentamiento por fricción en el seno del disco, la línea de hielo de nuestro sistema solar se encontraba inicialmente bastante más allá de la órbita de Júpiter. Fue desplazándose gradualmente hacia el interior al disminuir el flujo de masa a través del disco e irse disipando el gas. Con el tiempo, la ubicación de la línea se estabilizó bastante, aunque la linde hielo-vapor debió de ir adelante y atrás dentro de un margen de entre 1 y 2 UA, que abarcaba una porción importante de la región comprendida entre Marte y Júpiter. Los cuerpos progenitores de los meteoritos del cinturón de asteroides se formaron a lo largo de varios millones de años. Durante esa época, la línea de hielo pudo haber invadido regiones cercanas a Marte. Consiguientemente, el contenido acuoso de los meteoritos aumentó gradualmente con la distancia al Sol de sus cuerpos progenitores. Esta evolución pudo haber favorecido la adquisición por la Tierra de sus océanos.*



La teoría de acreción secuencial, la principal hipótesis acerca de la formación de los planetas, entraña una interacción caótica entre diversos mecanismos en competencia, como la reubicación de la línea de hielo, lo que origina una gran diversidad de resultados.

Recopilación de Daniel C. Schlenoff

...cincuenta años

Información y política. «La escuela soviética de genética dirigida por Trofim D. Lysenko parece que ha vuelto a renacer. Se esperaba que en el Congreso Internacional de Genética de Montreal la URSS estuviera representada por varios genetistas no lysenkonianos, pero no vino ninguno. Tal ausencia y la presentación a última hora de varios trabajos dieron a la reunión un sabor inconfundiblemente lysenkoniano. El Congreso adoptó una resolución que condenaba 'todo intento por parte de los gobiernos de interferir por razones políticas, ideológicas o de otra índole en la libre búsqueda científica y la libre difusión de la ciencia.'»

El precio a pagar. «En los tramos más profundos de un pozo de 6000 metros, el costo total del mismo supera ya el millón de dólares. Con el petróleo crudo a 3 dólares el barril, el pozo debe producir lo suficiente para justificar su explotación. Cuando se trata de perforaciones de prospección, esos costos parecen aún más imponentes. El record mundial de profundidad de 7600 metros parece fijar el límite económico de los métodos de perforación actuales. Pero en algunas zonas el espesor de los depósitos de rocas sedimentarias supera los 12.000 metros, y parece que no hay razones geológicas para que no pueda encontrarse petróleo a tan enormes profundidades. Si hay que satisfacer la creciente demanda de productos petrolíferos, deben hallarse procedimientos de prospección y extracción en esas formaciones profundas.»

...cien años

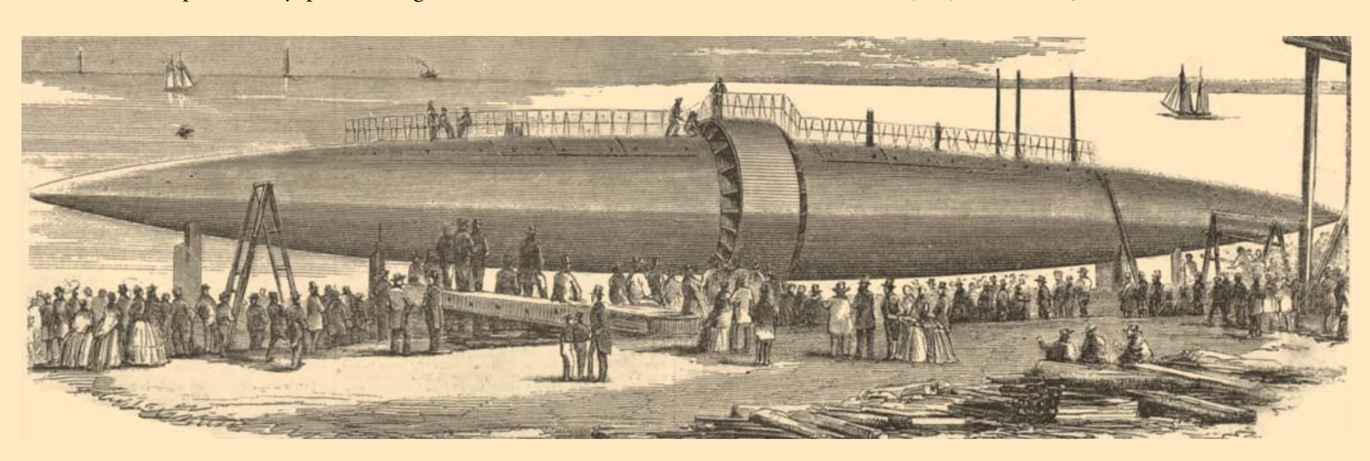
Un trabajo delicado. «Se ha logrado dividir en once piedras el famoso diamante Cullinan. En cierto modo el diamante era un elefante blanco: demasiado grande y valioso para hallar un comprador. El problema de qué hacer con él desconcertaba no poco a la empresa. Finalmente se presentó la piedra al rey Eduardo, quien decidió confiar a una firma de Amsterdam su partición y pulido. Según el *London Times*, en su estado original el diamante Cullinan pesaba casi 600 gramos. Si bien un brillante suele tener cincuenta y ocho facetas, en vista de su inmenso tamaño al Cullinan se le dieron setenta y cuatro. Tal decisión ha resultado sobradamente justificada por los resultados.»

...ciento cincuenta años

Hágase la luz. «Sir James Wylie, difunto médico del emperador de Rusia, dedicó gran atención al estudio de los efectos de la luz como agente curativo en los hospitales de San Petersburgo. Descubrió que el número de pacientes que sanaban en las salas bien iluminadas cuadruplicaba el número de los que sanaban en salas obscuras. Así se precipitó la reforma radical de la iluminación de los hospitales rusos, con resultados óptimos, merced a la acción de la luz, sin cuya abundancia la vida de plantas y animales no es sino enfermiza y precaria. Las estadísticas sanitarias de todos los países civilizados han mejorado mucho a lo largo del siglo pasado. Ello podría responder a una mejor construcción de los edificios, que dejan penetrar más luz en el interior.»

El buque cigarro. «Hace dos semanas dimos noticia del original buque de vapor en curso de construcción por los señores Winans, de Baltimore (Maryland). Ofrecemos ahora una vista del mismo tomada de una fotografía. Las hélices están dispuestas entre ambas mitades de la embarcación, protegidas por un manguito o guarda, de los daños que pudieran producir maderos, cuerpos flotantes o los muelles a los que estuviera atracada. Al casco se añadirán las tomas de ventilación, las chimeneas y la caseta de navegación. Tal es la construcción de este buque sin velas; si las máquinas sufren algún accidente quedará como un tronco abandonado a merced de las olas. Por muy fuertemente que sus partes se afiancen, su forma es inestable, como cualquiera puede apreciar en el movimiento de un barril sobre las olas o en aguas encrespadas.»

[NOTA: El buque, diseñado para viajar en superficie, incorporaba algunas ideas innovadoras; con todo y a pesar de extensas modificaciones, nunca fue apto para la navegación.]



EL BARCO DE VAPOR WINANS, durante su construcción en 1858.

SCIENTIFIC AMERICAN, VOL. XIV, N.º 9; 6 DE NOVIEMBRE DE 1858

¿Qué ha sido de ...?

Recopilación de Philip Yam

Protección joviana

Júpiter, el primero de los planetas que se formó en nuestro sistema solar, contribuyó a esculpir a los demás [*véase* “La génesis de los planetas”, en INVESTIGACIÓN Y CIENCIA, julio de 2008]. Su gravitación ha regulado la tasa de impactos cósmicos en la Tierra: unas veces lanzando como una honda asteroides en nuestra dirección y otras atrayendo hacia sí y apartando de nuestro camino rocas espaciales peligrosas. Jonathan Horner y Barrie Jones, de la Universidad a Distancia del Reino Unido, proponen, en un artículo de próxima publicación en *International Journal of Astrobiology*, que este efecto joviano es consecuencia de la masa del planeta. Si Júpiter tuviera una quinta parte de su masa, no hubiera podido apartar tantos asteroides y se habría cuadruplicado el número de impactos recibidos en la Tierra. Si Júpiter hubiera sido más pequeño aún, habría desviado todavía menos asteroides hacia el sistema solar interior. (Los dinosaurios quizá seguirían hollando nuestro planeta.)

—*George Musser*

MEDICALRF.COM (ventilador); KUAKO HELAVUO (Júpiter y asteroide); FLIP NICKLIN Minden Pictures (leones marinos varados)

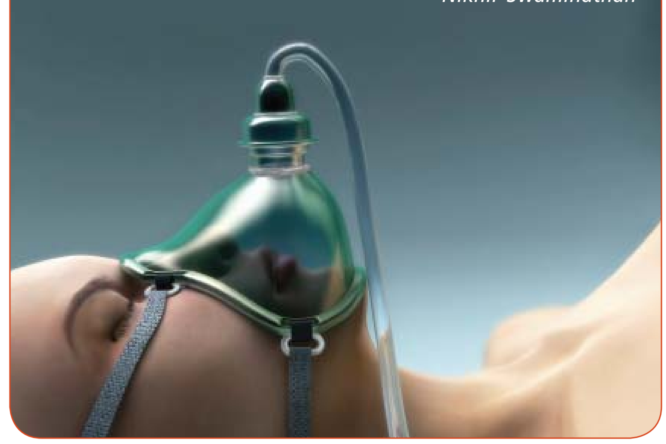


1. EL TAMAÑO IMPORTA. Por su masa, Júpiter atrae hacia sí a numerosos asteroides.

Inconsciencia dolorosa

La anestesia general deja al paciente inconsciente mediante la desconexión del sistema nervioso central [*véase* “Hacia una anestesia más segura” en INVESTIGACIÓN Y CIENCIA, agosto de 2007]. En el hospital de la Universidad de Georgetown se ha descubierto que los anestésicos interactúan también con proteínas específicas de la superficie de las neuronas, de forma que podría aumentar el dolor del paciente al recuperar la consciencia. Estudios con ratones indican que fármacos activadores de la proteína superficial TRPA1 de las neuronas sensoras del dolor intensifican el dolor postoperatorio. Ello explicaría por qué unos pacientes se quejan de dolores más intensos que otros que se han sometido a la misma intervención quirúrgica. En el futuro, los anestesistas podrían reducir el dolor postoperatorio ciñéndose a anestésicos que no interaccionen con TRPA1. El trabajo figura en el número de 24 de junio de *Proceedings of the National Academy of Sciences USA*.

—*Nikhil Swaminathan*



Prohibido leer ADN

Numerosos investigadores ponen en duda la relevancia médica de los análisis genéticos que se ofrecen directamente al consumidor por sólo 1000 dólares. Parece que el gobierno norteamericano opina lo mismo. En junio, el Departamento de Salud Pública de California, invocando las normas de licencia y supervisión médica, remitió notificaciones a 13 laboratorios de ensayos de ADN para que cesaran de solicitar clientes, entre ellos 23andMe, Navigenics y deCODEme. Estas órdenes de “cese y renuncia” llegan después de que el estado de Nueva York comenzase a enviar notificaciones similares en noviembre de 2007. Dichas cartas constituyen, en parte, un intento de establecer mecanismos de supervisión federal para este sector naciente; se teme que haya personas que reaccionen de forma inadecuada al conocer sus riesgos de padecer enfermedades.

—*Philip Yam*

Daños y perjuicios

Los estudios que han evaluado el impacto ambiental a largo plazo de los vertidos en el desastre del *Exxon Valdez* en 1989 han estado rodeados de controversia. Según una decisión del Tribunal Supremo estadounidense del 25 de junio, la gigantesca petrolera ExxonMobil deberá pagar a los perjudicados por las 37.000 toneladas de crudo derramadas en Prince William Sound (Alaska) el equivalente al valor de las ventas de petróleo correspondientes a 24 horas. Esta decisión estima que los daños totales imputables a la compañía son de 507,5 millones de dólares, aproximadamente la décima parte de los 5000 millones que inicialmente un jurado concedió a los querellantes en 1994. El Tribunal decidió, por mayoría, que las sanciones e indemnizaciones habrían de estar en correspondencia con los daños demostrados, sentando así nueva jurisprudencia para los desastres marítimos por vertidos de buques petroleros.

—*David Biello*



2. CRUDO EN EL MAR. Varios leones marinos se refugian en una boya. Huyen del petróleo vertido por el *Exxon Valdez* en Prince William Sound en 1989.

IMAGENES CEREBRALES

¿Qué ves?

Un grupo de científicos de la Universidad de California en Berkeley ha desarrollado un método dotado de capacidad para descodificar los patrones de activación de las áreas visuales del cerebro y determinar así lo que una persona ha visto. Utilizaron la técnica de la resonancia magnética funcional para registrar la actividad en la corteza cerebral de unos voluntarios que tenían que mirar una serie de imágenes. Los investigadores dedujeron qué imagen estaban viendo esas personas observando la actividad en diferentes secciones del cerebro y descifrando qué tipo de información debía de haber en la parte correspondiente del campo visual. Sin embargo, el método se limita al desciframiento de información que admita representación matemática, como imágenes, sonidos y movimientos.

—Nikhil Swaminathan



LA RESONANCIA MAGNETICA funcional permite cierta forma de lectura de la mente.

ECOLOGIA

Arboles escaladores

Unas dos terceras partes de las especies forestales de seis sierras francesas han ascendido al menos 18,5 metros por las laderas de las montañas por cada década del siglo XX. Por investigaciones anteriores se sabía que las plantas de los puntos más elevados de las montañas y de las regiones polares se han desplazado para adaptarse al calentamiento global. La comprobación francesa es la primera de que también en altitudes más bajas y con climas más suaves se están moviendo ecosistemas enteros.

—David Biello

EVOLUCION

Ojos de rodaballo

La extraña metamorfosis de fletanes, rodaballos, platijas y otros peces planos hizo que hasta Darwin se las viese y desease para darle explicación. Al nacer, estos peces tienen un ojo a cada lado del cráneo, pero en la edad adulta ambos se hallan arriba. Sin duda, para peces que pasan toda la vida en el fondo del mar tener los dos ojos mirando hacia arriba supone una ventaja. Pero no parecía haber razón evolutiva alguna para iniciar el cambio gradual hacia tal asimetría; las posibles etapas intermedias no parecen ser especialmente ventajosas. Algunos biólogos apoyan la teoría de que estos peces evolucionaron a partir de una única mutación súbita.

Esta teoría parece errónea: Matt Friedman, del Museo Field de Chicago, ha encontrado algunos eslabones perdidos. Investigó dos fósiles de peces planos primitivos de hace unos 50 millones de años, ocultos en museos europeos desde hace más de un siglo. Estos ejemplares adultos poseen cráneos algo asimétricos que, sin embargo, mantienen los ojos a ambos lados de la cabeza. Friedman sugiere que incluso una asimetría parcial puede haber dado a los habitantes carnívoros del fondo marino una mejor visión de sus alrededores que la ausencia total de asimetría.

—Charles Q. Choi



DATOS

TV de efecto invernadero

Fabricar televisores, al parecer, puede ser perjudicial para el clima. Para fabricar las pantallas planas se emplea trifluoruro de nitrógeno (NF_3), un gas de potente efecto invernadero. Este gas no está cubierto por la regulación de emisiones del Protocolo de Kyoto de 1997, porque apenas se utilizaba entonces. Ahora, la explosión de ventas de televisores de pantalla plana y otros dispositivos digitales, junto con una recuperación incompleta de los agentes químicos durante la fabricación, podría suponer un problema, advierten Michael J. Prather y Juno Hsu, de la Universidad de California en Irvine. Abogan por una investigación en profundidad para documentar la presencia de NF_3 en la atmósfera.



Vida media en la atmósfera del NF3: 550 años

Factor de potencia de efecto invernadero (potencial de calentamiento climático), en comparación con el dióxido de carbono, del

Metano: 25

NF_3: 17.200

Cantidad estimada de producción de NF_3 en 2008: 4000 toneladas

Cantidad equivalente de CO_2, en toneladas: 67 millones

Porcentaje de NF_3 no recuperado durante la producción: entre 2 y 3

Emisiones de CO_2 en 2005, en toneladas: 15.128 millones

FUENTE: Geophysical Research Letters, *26 de junio de 2008*

JOHN-FRANCIS BOURKE *zefa/Corbis (arriba a la izquierda)*; MATT COLLINS *(derecha)*; SCOTT LESLIE *Minden Pictures (rodaballo)*

BIOLOGIA

¿Cuánto tiempo persiste el metabolismo celular tras la muerte?

En la medida en que tal determinación resulta posible, el metabolismo celular prosigue entre 4 y 10 minutos después de la muerte, aproximadamente, dependiendo de la temperatura del ambiente en que se encuentre el cadáver.

Durante este intervalo, la sangre oxigenada, que normalmente intercambia dióxido de carbono y oxígeno, no está circulando. La acumulación de dióxido de carbono producido por la respiración celular reduce el *p*H de las células; o lo que es igual, el medio intracelular se torna más ácido.

La acidez de este ambiente provoca la rotura de las membranas intracelulares, entre ellas las que envuelven los lisosomas de las células, corpúsculos que contienen enzimas capaces de digerirlo todo, desde las proteínas y las grasas hasta los ácidos nucleicos. Al romperse las membranas, las enzimas liberadas comienzan una digestión de las células desde su interior, la autolisis, o autodigestión.

Células hepáticas

La velocidad de difusión autolítica depende de la densidad local de enzimas; en el tejido hepático, que es rico en estas proteínas, la velocidad es probablemente mayor que en el tejido pulmonar, cuya reserva enzimática es menor. La autolisis progresa más rápidamente también en los tejidos ricos en agua, como es el caso de los tejidos cerebrales.

La temperatura ambiente desempeña una función más crítica todavía en la regulación de la difusión autolítica. En ambientes cálidos este proceso autodigestivo se acelera, mientras que el frío lo retarda. Por esta razón, ha sido posible reanimar a personas ahogadas en agua muy fría incluso trascurridos períodos bastante largos. En tales casos, el proceso autolítico se ha visto retardado por el frío y ello ha impedido que los tejidos sufran daños permanentes.

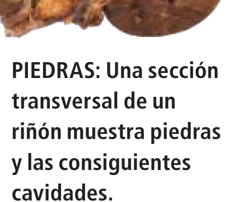
—*Arpad Vass*,
antropólogo forense, Laboratorio Nacional de Oak Ridge

CLIMA Y SALUD

La nueva Edad de Piedra

La prevalencia de los cálculos renales aumentará en el siglo XXI en un mundo que se calienta, según Tom H. Brikowski, de la Universidad de Texas en Dallas, y sus colaboradores. Las piedras, que son cristalizaciones de los minerales disueltos en la orina, se pueden formar por la pérdida de fluidos. Tal deshidratación es más común en los climas más calientes; por ejemplo, la incidencia en el sureste de EE.UU. es un 50 por ciento mayor que en la región noroeste del país. Algunos soldados estadounidenses enviados a climas desérticos desarrollaron piedras a los 90 días del despliegue. Teniendo en cuenta el aumento previsto en la temperatura media en los EE.UU., un aumento de entre dos y cinco grados en este siglo, los investigadores calculan que la nación sufrirá entre 1,6 millones y 2,2 millones más de casos de cálculos renales en el año 2050. Este aumento de entre el 7 y 10 por ciento podría suponer 1300 millones de dólares de gasto médico.

—*Philip Yam*



PIEDRAS: Una sección transversal de un riñón muestra piedras y las consiguientes cavidades.

DAVID McCARTHY *Photo Researchers, Inc. (células hepáticas)*; E. WALKER *Photo Researchers, Inc. (piedras del riñón)*; ANUP SHAH *NPL/Minden Pictures (chimpancés)*

INFECCIONES

Jugando con gérmenes

Los niños que van a la guardería y a la escuela se contagian frecuentemente entre ellos enfermedades respiratorias. Las comunidades de chimpancés parecen sufrir un fenómeno similar: los juegos en grupo facilitan la difusión de infecciones respiratorias entre los primates, según un nuevo estudio.

Un grupo de científicos dirigido por Hjalmar Kuehl y Peter Walsh, del Instituto Max Planck de Antropología Evolutiva de Leipzig, examinó dos grupos de chimpancés del Parque Nacional de Taï, en Costa de Marfil. Los chimpancés jóvenes tenían mayores probabilidades de morir de una enfermedad respiratoria cuanto más jugaban en grupo, generalmente durante la temporada de las frutas, cuando esos animales se reúnen. Entre los dos y los tres años, los chimpancés pasan hasta el 18 por ciento del tiempo en contacto físico con sus compañeros. Este período es para ellos el de mayor interacción social y sirve para unir a los miembros de la comunidad.

Una vez que los chimpancés juguetones produjeron un brote, las crías de todas las edades contrajeron la enfermedad y perecieron. Las madres afectadas rápidamente entraron en celo, perpetuando el ciclo de tres años de aumento y caída de la población infantil. Junto con la caza furtiva, el cambio climático y la depredación por parte de otros animales, la mortalidad infantil por enfermedades infecciosas está afectando gravemente a los chimpancés de la zona, afirma Kuehl. Hoy en día pocos bebés llegan a la edad adulta, afirma: "Sólo cuatro de cada diez llegan a los cinco años de edad."

—*Barbara Juncosa*



JUGAR en grupo ayuda a los jóvenes chimpancés a desarrollar habilidades sociales, pero también propaga enfermedades contagiosas.

Convergencia evolutiva

El panda gigante y el panda rojo comparten un "falso pulgar". Aunque parezca la consecuencia de una estrecha relación de parentesco, la coincidencia se debe a una convergencia evolutiva

Damos el mismo nombre de "panda" a dos especies de carnívoros distintas, el panda gigante (*Ailuropoda melanoleuca*) y el panda rojo (*Ailurus fulgens*). El primero pertenece a la familia de los úrsidos. El segundo, poco mayor que un gato doméstico), se incluye en la familia de los ailúridos. Amén de una cara redondeada con un vistoso "antifaz" oscuro, ambos presentan importantes rasgos en común. Se alimentan de bambú y poseen una particularidad anatómica que les diferencia del resto de los carnívoros: un hueso hipertrofiado que opera a modo de "falso pulgar" y les facilita la manipulación de los brotes de bambú.

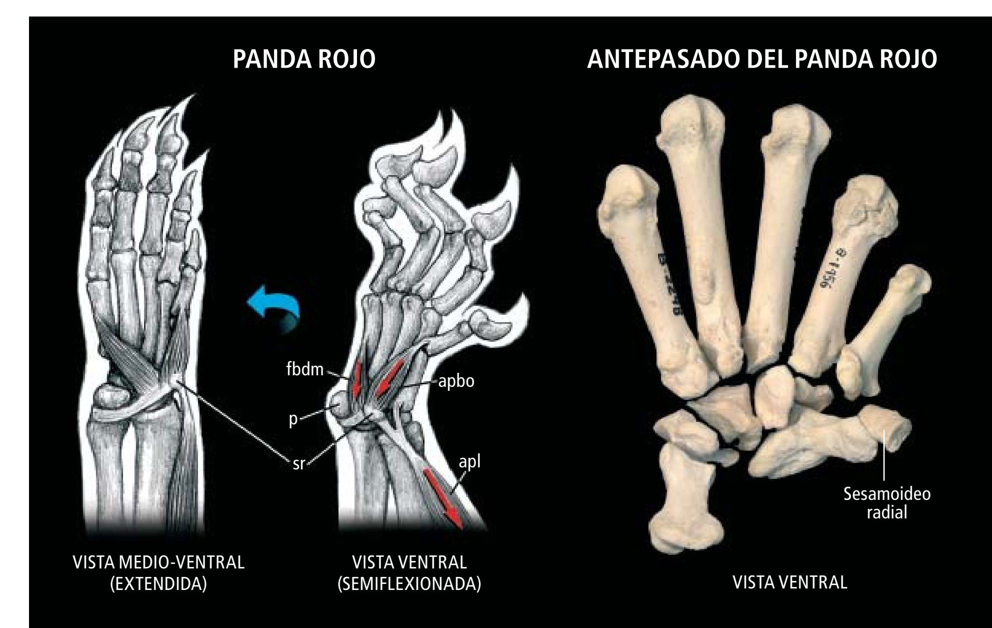
Ese hueso está presente, aunque muy reducido, en numerosas especies carnívoras. Pero sólo en los pandas muestra un desarrollo suficiente para participar en la función prensil de la mano. ¿Por qué evolucionó esa estructura en los pandas? Al contrario que el de los primates, el pulgar (verdadero) de los carnívoros no diverge de los otros dígitos, con la limitación consiguiente de la capacidad prensil. Para superar esa desventaja, se desarrolló uno de los pequeños huesos sesamoideos de la zona de la muñeca, que en origen servía para amortiguar la fricción entre tendones y huesos en las zonas de articulación; su nueva función le permitía girar respecto de la palma de la mano, con lo que imitaba el efecto del pulgar oponible de los primates.

La presencia del "falso pulgar" en ambos pandas indujo a pensar en un estrecho parentesco entre ambas especies. Hasta que la investigación sacó a la luz que tal coincidencia correspondía a una convergencia evolutiva. En un principio se supuso que ambos animales habían desarrollado, a partir de antepasados carnívoros, una dieta especializada en el bambú, que habría requerido una mayor capacidad prensora de las manos.

Pero esa hipótesis ha sido desmentida por el hallazgo en el yacimiento madrileño de Batallones-1 de fósiles muy completos de un pariente extinguido del panda rojo que ya poseía un falso pulgar: *Simocyon batalleri*, un carnívoro del tamaño de un puma. La dentición de *Simocyon* indica que se alimentaba sobre todo de carne; por tanto, el falso pulgar no lo aplicaba a la manipulación del bambú, sino a la locomoción arborícola, para la cual mostraba evidentes adaptaciones en el resto del esqueleto.

Los fósiles de Batallones-1 arrojan nueva luz sobre el origen del falso pulgar en la familia del panda rojo. En contra de la hipótesis inicial, no fue el consumo de bambú lo que favoreció la aparición de ese rasgo, sino la capacidad de trepar en los árboles. La adaptación se produjo en miembros más antiguos de la familia que no habían desarrollado la dieta vegetariana del panda rojo actual.

El equipo de paleontólogos del Museo Nacional de Ciencias Naturales y la Universidad de Poitiers que estudió el *Simocyon* de Batallones-1 ha ido un paso más allá. En colaboración con el anatomista Juan Francisco Pastor, de la Universidad de Valladolid, han diseccionado y estudiado, mediante un escáner

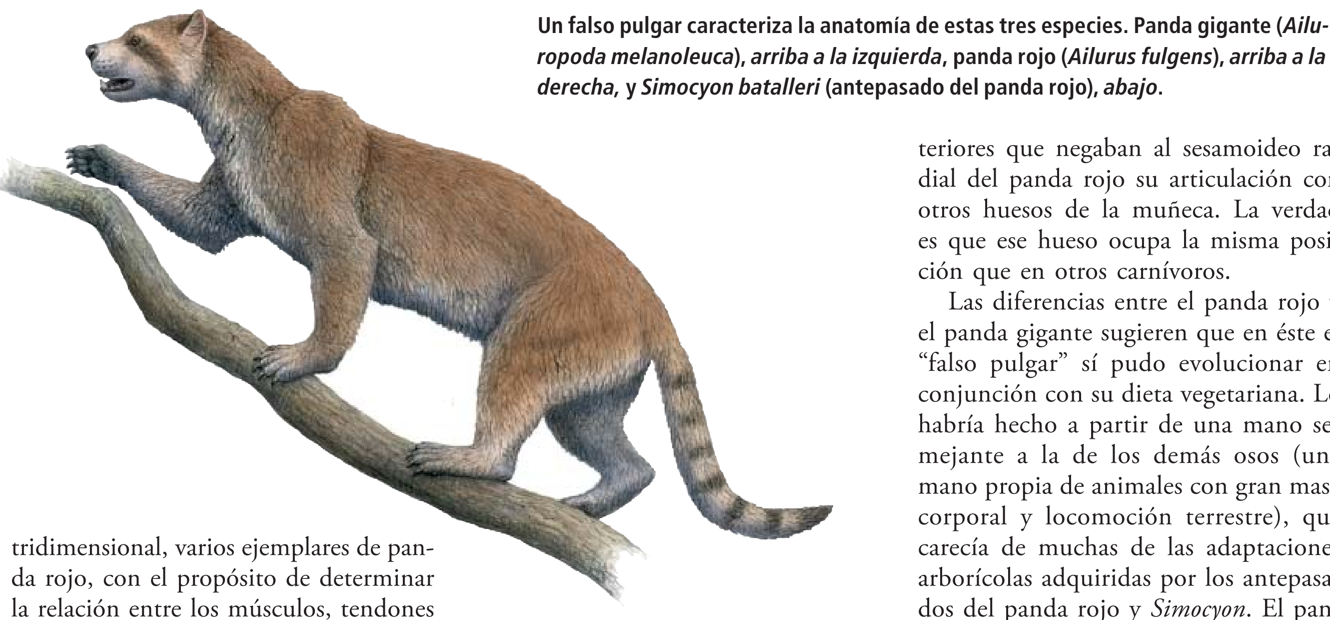


Los pandas poseen un rasgo anatómico particular: un falso pulgar que contribuye a la acción prensil de la mano. La ilustración muestra los huesos y los músculos de la mano derecha de un panda rojo (*Ailurus fulgens*). Las flechas (*rojo*) señalan el sentido en el que tiran las fibras musculares durante la contracción. La flecha central (*azul*) indica el sentido de rotación de la mano debida a la acción supinadora del *abductor pollicis longus* (*apl*), el principal músculo que acciona el "falso pulgar" o sesamoideo radial (*sr*). Se muestran también los músculos *abductor pollicis brevis* y *oppones pollicis* (*apbo*), *flexor brevis digitorum manus* (*fbdm*) y el hueso pisiforme (*p*).

El falso pulgar se ha descubierto también en un pariente del panda rojo que vivió en el mioceno superior (*Simocyon batalleri*). La fotografía corresponde al carpo y metacarpo derechos de este mamífero extinguido. Se alimentaba de carne y carroña, por lo que el falso pulgar no lo aplicaba a la manipulación del bambú sino a la locomoción arborícola, para la cual muestra adaptaciones en el resto del esqueleto. La presencia del sesamoideo radial en este carnívoro trepador confirma la relación entre la locomoción arborícola y la aparición en los ailúridos del falso pulgar.







Un falso pulgar caracteriza la anatomía de estas tres especies. Panda gigante (*Ailuropoda melanoleuca*), *arriba a la izquierda*, panda rojo (*Ailurus fulgens*), *arriba a la derecha,* y *Simocyon batalleri* (antepasado del panda rojo), *abajo*.

tridimensional, varios ejemplares de panda rojo, con el propósito de determinar la relación entre los músculos, tendones y huesos en la mano. Los resultados obtenidos nos permiten ahondar en la evolución de esos carnívoros.

Los resultados confirman la relación entre la locomoción arborícola y la aparición en los ailúridos del falso pulgar. En el panda rojo, el sesamoideo radial se halla menos desarrollado que en el panda gigante; cuenta con una conexión (mediante tendones) con los músculos flexores de la mano, que aumenta su contribución a la acción prensil de ésta. Además, el principal músculo que acciona al "falso pulgar", el *abductor pollicis longus*, presenta en ese animal una inserción en el primer metacarpiano, lo que contribuye a la supinación. Ese modelo de "mano prensil" guarda semejanza con el que se observa en microcarnívoros arborícolas, si bien ninguno posee un sesamoideo radial tan desarrollado como el panda rojo.

La cabal precisión de esas observaciones permite refutar interpretaciones anteriores que negaban al sesamoideo radial del panda rojo su articulación con otros huesos de la muñeca. La verdad es que ese hueso ocupa la misma posición que en otros carnívoros.

Las diferencias entre el panda rojo y el panda gigante sugieren que en éste el "falso pulgar" sí pudo evolucionar en conjunción con su dieta vegetariana. Lo habría hecho a partir de una mano semejante a la de los demás osos (una mano propia de animales con gran masa corporal y locomoción terrestre), que carecía de muchas de las adaptaciones arborícolas adquiridas por los antepasados del panda rojo y *Simocyon*. El panda rojo, por su parte, sigue siendo hoy en día un hábil trepador: se desplaza con facilidad entre las ramas y es capaz de descender cabeza abajo por un tronco vertical, una hazaña al alcance de pocos carnívoros.

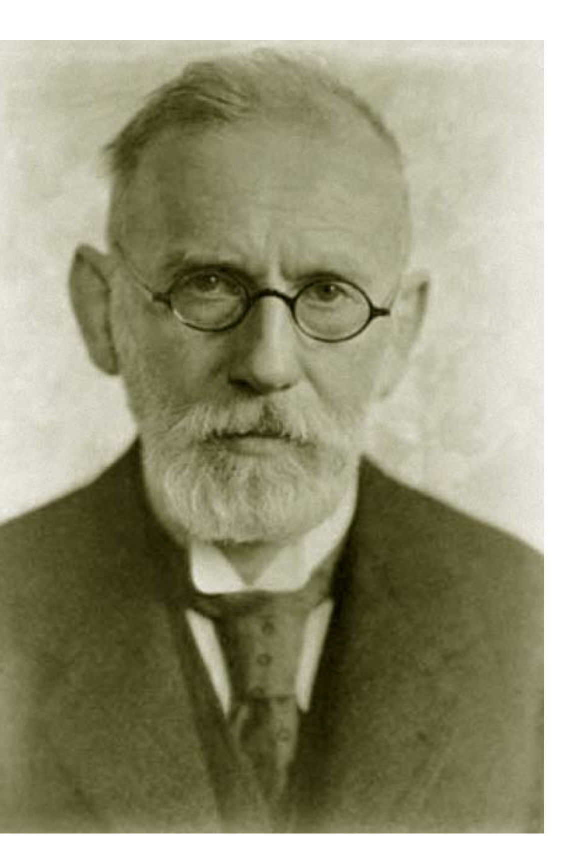
Mauricio Antón, Manuel J. Salesa
y **Jorge Morales**
Departamento de Paleobiología.
Museo Nacional de Ciencias Naturales,
CSIC, Madrid

Paul Ehrlich

De la quimioterapia a la inmunología. Centenario de un premio Nobel

En 1878, el joven médico alemán Paul Ehrlich presentó una novedosa tesis doctoral sobre las "tinciones vitales". En ella analizaba el efecto singular de ciertos colorantes, que mostraban la capacidad de ser incorporados selectivamente por los tejidos vivos. Después de estudiar la afinidad, composición química y modo de acción de numerosas sustancias, Ehrlich obtuvo un primer éxito en el tratamiento de la malaria con azul de metileno. El método mostraba cierta eficacia, pero no la suficiente como para aceptar su utilización clínica.

Sin embargo, ese trabajo le permitió desarrollar el concepto de quimioterapia, basado en la utilización de moléculas tóxicas que se unían específicamente a los microorganismos patógenos y ejercían su acción antiséptica, a la vez que respetaban la integridad del hospedador.



Paul Ehrlich (1854-1915) fundó la quimioterapia a partir de las "balas mágicas", moléculas tóxicas que se unían de forma específica a los microorganismos patógenos, a la vez que respetaban la integridad del hospedador. Por sus trabajos sobre la inmunidad, recibió junto con Ilya Mechnikov el premio Nobel de medicina en 1908.

La cualidad esencial de "una bala mágica" debía ser, pues, la toxicidad selectiva contra el agente infeccioso y no la potencia antimicrobiana.

El trabajo persistente de Ehrlich y sus colaboradores K. Shiga y A. Bertheim sirvió para encontrar un nuevo colorante, el rojo tripán, eficaz en el tratamiento de la tripanosomiasis y otras enfermedades de origen protozoario. No obstante, el mayor logro del laboratorio se obtuvo tras la exploración exhaustiva de un remedio contra la espiroqueta que causaba la sífilis; buscaban una sustancia que evitara las complicaciones causadas por las terapias entonces al uso. Los mejores candidatos iniciales fueron los óxidos de arsénico (atoxyl). Inicialmente mostraban ciertos efectos secundarios indeseables, pero su modificación mediante síntesis química dio lugar a un conjunto de derivados más seguros y efectivos en el control de la sífilis, que culminaron con el hallazgo del famoso Salvarsan 606.

Ehrlich fue también pionero en la introducción de nuevos conceptos y técnicas de uso imprescindible en la quimioterapia actual. Por ejemplo, el muestreo simultáneo de numerosos compuestos potencialmente interesantes, su ensayo mediante pruebas sencillas y su posterior modificación estructural para obtener derivados con mejor actividad biológica y menor toxicidad. Demostró el modo en que algunos fármacos experimentaban activación metabólica dentro del cuerpo. Otras sustancias, antibacterianas y antifúngicas, controlaban la infección sin matar al patógeno; para éstas acuñó el término "bioestático" (en contraposición a "biocida").

A principios del siglo pasado, Ehrlich detectó el problema incipiente de la resistencia que presentaban ciertos microorganismos frente a la quimioterapia. En la actualidad, las cepas multirresistentes a los antibióticos constituyen el principal desafío para los sistemas de salud pública del primer mundo.

Tras su fallecimiento en 1915, las ideas de Ehrlich fueron en gran medida abandonadas. Se consideraba que los antibióticos servían sólo para potenciar las defensas del organismo, pero que carecían de utilidad clínica. Hubo que esperar hasta los trabajos de G. Domagk con las sulfamidas primero, y de A. Fleming, E. B. Chain y H. Florey con la penicilina después, para que la microbiología conociera una segunda edad de oro, cuyas enormes repercusiones sociales alcanzan hasta nuestros días.

Además de otras aportaciones relevantes a los campos de la histoquímica y la hematología, Ehrlich trabajó intensamente sobre los mecanismos defensivos de los mamíferos frente a la agresión de patógenos externos. Como corolario de sus investigaciones, formuló la teoría de "la cadena lateral", que explicaba la síntesis de anticuerpos y la especificidad de la respuesta inmunitaria.

Según esta hipótesis, las células inmunitarias (linfocitos) poseen receptores únicos y altamente específicos (cadenas laterales) unidos a la superficie de su membrana citoplásmica. Dichos receptores reconocen y se unen exclusivamente a ciertos grupos químicos de la toxina o antígeno (epitopos). La unión desencadena la producción masiva de cadenas laterales, que son liberadas mayoritariamente a la sangre en forma de antitoxinas circulantes (anticuerpos). Una parte de los linfocitos conserva memoria de su primer contacto con los antígenos extraños, lo que asegura una respuesta más contundente en futuros encuentros.

Se cumple este año el centenario de la concesión a Ehrlich del premio Nobel de Medicina, que compartió con el científico de origen ucraniano Ilya Mechnikov en reconocimiento por sus trabajos sobre la inmunidad.

Juan Carlos Argüelles
Area de Microbiología
Universidad de Murcia

Tragados por el Sol

Sí, el Sol terminará por engullir a la Tierra... quizá.

El Sol se expande e intensifica su luminosidad poco a poco. En unos miles de millones de años terminará por desecar la Tierra, que se convertirá en un planeta caliente, marrón e inhabitable. De aquí a unos 7600 millones de años, alcanzará su máximo tamaño, convertido en gigante roja: su superficie sobrepasará la órbita actual de la Tierra en un 20 por ciento y su luz será 3000 veces más intensa. Luego, el Sol entrará en su fase terminal: se hundirá sobre sí mismo y se transformará en una enana blanca.

Si bien hay coincidencia en lo concerniente al Sol, se discrepa por lo que le ocurrirá a la Tierra. Desde que en 1924 el matemático británico James Jeans pensara en la suerte del planeta durante la fase de gigante roja de su estrella, se han formulado hipótesis vario-

pintas. Según varios modelos, la Tierra escapa de la vaporización; en los análisis más recientes, sin embargo, no es así.

La respuesta no es inmediata porque, aunque el Sol se expandirá más allá de la actual órbita de la Tierra —que mide una "unidad astronómica" (UA)—, también perderá masa por el camino: para cuando alcance el máximo radio de 1,2 UA, el Sol habrá perdido una tercera parte de su masa, en comparación con su estado actual. La atracción gravitatoria, pues, será menor, y la Tierra se desplazará hacia fuera. Podría escapar así de la envoltura solar.

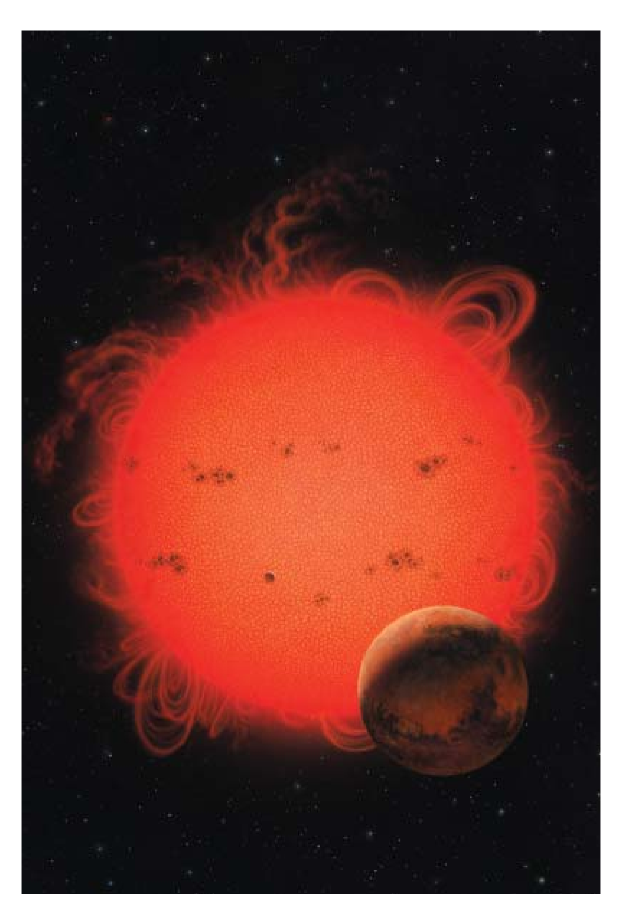
Pero existen otros factores que complican el análisis. El rozamiento del planeta con las capas más tenues y exteriores del Sol hará que vuelva a caer hacia el Sol. Resulta aún más difícil predecir las pequeñas fuerzas ejercidas por los demás planetas, todos a su vez reaccionando ante un mismo Sol en expansión.

A principios de este año, dos equipos anunciaron cálculos diferentes que presagian que la Tierra será absorbida por el Sol. Lorenzo Iorio, del Instituto Nacional Italiano de Física Nuclear, aplicó la teoría de perturbaciones. Los análisis se simplifican eliminando pequeños factores; las complejas ecuaciones del movimiento que detallan las interacciones entre el Sol y la Tierra se vuelven así manejables matemáticamente. Bajo el supuesto de que la pérdida anual de masa solar seguirá siendo tan escasa como hoy (una parte en 100 billones) durante la evolución hacia la fase de gigante roja, Iorio determina que la Tierra se desplazará hacia fuera a un ritmo de 3 milímetros por año, un total de apenas 0,0002 UA para cuando el Sol se convierta en una gigante roja. Llegado ese momento, el Sol se inflará en apenas un millón de años hasta alcanzar un radio de 1,2 UA: vaporizará la Tierra.

Hay dudas de que las cantidades que Iorio presupone pequeñas vayan a permanecer así a lo largo de la evolución del Sol. Pero incluso aunque no sea así, es posible que Iorio haya dado con la respuesta correcta. En un análisis publicado en el número de mayo de 2008 de la revista *Monthly Notices of the Royal Astronomical Society*, Klaus-Peter Schröder, de la Universidad de Guanajuato, y Robert Smith, de la Universidad de Sussex, llegaban también a la conclusión de que la Tierra está condenada. Emplearon modelos solares más precisos y tuvieron en cuenta las interacciones de marea. A la vez que el Sol pierde masa y se expande, la rotación se frena, por la conservación del momento angular. Una menor rotación produce en la superficie solar una protuberancia de marea. La fuerza de gravedad ejercida por esta protuberancia atraería a la Tierra hacia el interior. Con este factor, Schröder y Smith calculan que los planetas que hoy día se encuentran a menos de 1,15 UA serán destruidos por el Sol.

Si, pese a todo, la Tierra tuviese para entonces todavía habitantes, ¿podrían salvarla? En un audaz ejercicio de ingeniería astronómica, Don Korycansky, de la Universidad de California en Santa Cruz, y sus colaboradores imaginan que se altere la órbita terrestre con un gran asteroide que pase cerca del planeta periódicamente. Se necesitarían mil millones de años para llevar nuestro planeta a algún lugar seguro, como la órbita de Marte. La Luna, sin embargo, tendría que quedarse atrás, y cualquier error de cálculo significaría la extinción.

David Appell



Sobrecalentado: Se debate si el Sol engullirá a la Tierra cuando se transforme en una gigante roja, dentro de miles de millones de años.

LYNETTE COOK *Photo Researchers, Inc.*

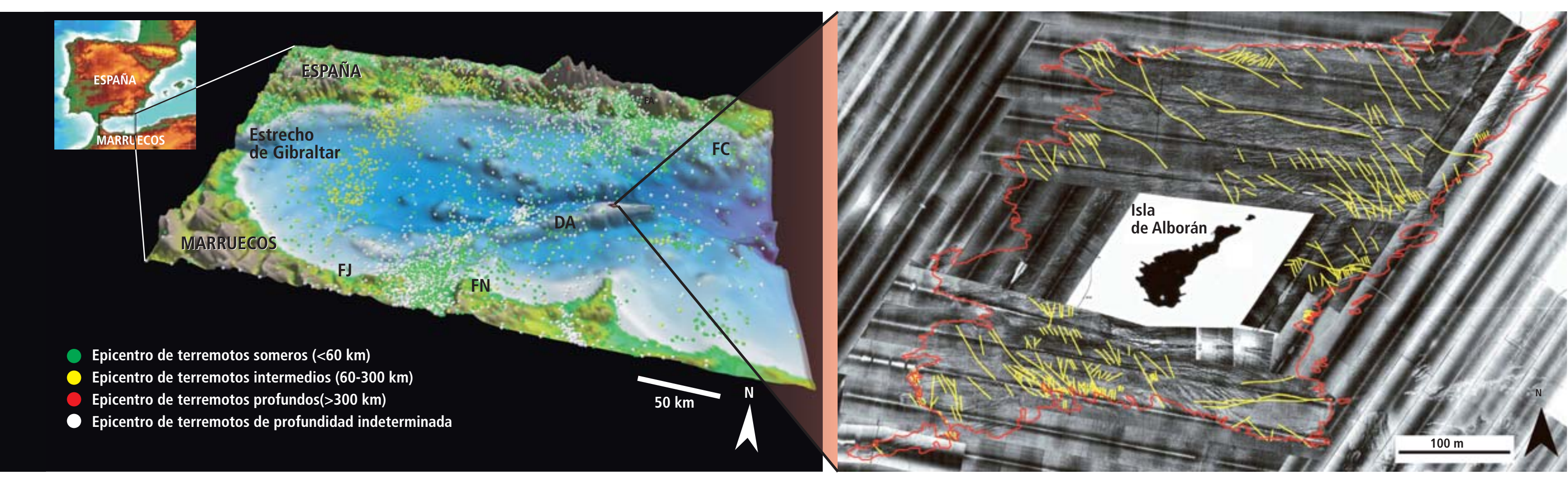
Fallas activas bajo el mar de Alborán

La reactivación de fallas antiguas bajo el campo de esfuerzos actual podría incidir en la génesis de terremotos en el mar de Alborán

El mar de Alborán corresponde a una de las áreas de España con mayor actividad sísmica. El estudio de los terremotos resulta vital para la evaluación del riesgo sísmico de la zona, así como para determinar las condiciones de habitabilidad y desarrollo de la actividad humana.

Este sector del margen meridional de la península Ibérica se halla en el límite entre las placas Euroasiática y Africana. Está delimitado por la cordillera Bética (sur de Iberia) y las cadenas del Rif y el Tell (norte de Africa), que constituyen el arco tectónico de Gibraltar.

La cuenca de Alborán presenta una estructura compleja, resultado de la superposición de varias fases tectónicas



Modelo digital del terreno del mar de Alborán y zonas emergidas limítrofes (*izquierda*). Se muestran los epicentros de los terremotos catalogados en el Instituto Geográfico Nacional; corresponden a los sucesos que han ocurrido desde 1487 hasta la actualidad. Se han identificado los principales elementos tectónicos con reflejo morfológico que presentan huellas de actividad sísmica reciente: falla de Jebha (FJ), falla de Nekor (FN), dorsal de Alborán (DA), falla de Carboneras (FC) y falla de Adra (FA). A la derecha, plataforma continental interna de la isla de Alborán. Esta imagen sonográfica obtenida mediante sonar de barrido lateral muestra el sustrato rocoso de origen volcánico (*contorno rojo*) intersectado por una serie de fallas (*amarillo*).

activas desde el Mioceno inferior (hace unos 20 millones de años o Ma) hasta la actualidad; se relacionan con el desarrollo del sistema orogénico bético-rifeño y con la evolución de las cuencas oceánicas del Mediterráneo Occidental. Tal complejidad ha quedado registrada no sólo en la formación de diversas estructuras tectónicas, sino también en la evolución del relleno sedimentario y en el desarrollo de procesos volcánicos.

Los modelos de la evolución de la cuenca muestran el modo en que las placas Africana y Euroasiática experimentaron un acercamiento N-S de 200 kilómetros entre el Oligoceno medio (28 Ma) y el Mioceno superior (11 Ma); le siguió una convergencia NO-SE de 50 kilómetros, con una tasa de movimiento de unos 5 milímetros anuales, desde el Tortoniense superior (9 Ma) hasta la actualidad. Esa convergencia ha resultado en un engrosamiento de la corteza continental de las cordilleras Bético-Rifeñas.

El mar de Alborán, en cambio, presenta una corteza continental adelgazada por extensión. La notable actividad sísmica del mar de Alborán se debe al movimiento de las fallas en respuesta a la convergencia entre las placas mencionadas. Los epicentros ofrecen una distribución amplia, a lo largo de una banda de unos 400 kilómetros de ancho. Algunos expertos consideran que ese patrón responde a una sismicidad difusa.

Un estudio realizado por investigadores del Instituto Geológico y Minero de España y del Instituto Español de Oceanografía, en el marco del Proyecto TOPOIBERIA, ha determinado, a partir del estudio de una imagen sonográfica de la plataforma continental de la isla de Alborán, la existencia de una serie de fallas que presentan una orientación preferente NO-SE a NNO-SSE.

La isla de Alborán corresponde a un relieve submarino que aflora por encima de la superficie del mar. Se halla sobre una dorsal de origen tectónico y con dirección NE-SO, que se prolonga hacia el sur hasta el margen marroquí. Se han descubierto otras fallas kilométricas paralelas a la dorsal de Alborán que se observan también en las zonas emergidas: Jebha y Nekor, en Marruecos, y Carboneras, en el sureste de la península Ibérica. Esta franja se denomina zona de cizalla Trans-Alborán; corresponde a una zona de fractura con comportamiento inverso-direccional de unos 100 kilómetros de ancho y 500 kilómetros de longitud.

El origen de las fallas de escala métrica a decamétrica que afectan a los materiales volcánicos del Mioceno superior (unos 9 Ma) del sustrato rocoso de la plataforma de la isla de Alborán guarda una estrecha relación con la reactivación, bajo el campo de esfuerzos actual, de estructuras geológicas antiguas de mayor escala. El análisis de las fallas de escala métrica a decamétrica que se observan en la imagen sonográfica ha permitido establecer el patrón de fracturación en función de su orientación y del sentido de movimiento de cada uno de los bloques. A partir de esa información, se ha establecido el modelo evolutivo que da lugar a su génesis.

Los resultados muestran que la formación de las fallas analizadas guarda relación con la reactivación de fallas de dirección NO-SE que compartimentan la dorsal de Alborán en bloques, y no con las grandes estructuras de dirección NE-SO que controlan la orientación de la dorsal. De este modo se ha definido la existencia de otras estructuras, de dirección casi ortogonal a la estructura principal, que podrían tener una incidencia relevante en la génesis de terremotos. La actividad de esas estructuras, algunas de las cuales controlan los rasgos morfológicos del fondo del mar de Alborán, da lugar a que se produzcan terremotos someros, a profundidades comprendidas en los primeros 60 kilómetros de la corteza.

Adolfo Maestro González
Area de Investigación en Cambio Global
Departamento de Investigación
y Prospectiva Geocientífica
Instituto Geológico y Minero de España

Patricia Bárcenas Gascón
Area del Medio Marino
y Protección Ambiental
Centro Oceanográfico de Málaga
Instituto Español de Oceanografía

Una nueva cacería de neutrinos

En el Fermilab confían en atisbar a un posible visitante de otras dimensiones

El hallazgo de nuevas dimensiones, que trasciendan de las cuatro a la que estamos habituados —tres para el espacio y una cuarta para el tiempo—, figuraría entre los descubrimientos más asombrosos de la historia de la física. En la actualidad, científicos del Laboratorio Nacional del Acelerador Fermi, el Fermilab, están diseñando un nuevo experimento para investigar unos indicios, tan alentadores como desconcertantes, de la posible existencia de dimensiones adicionales.

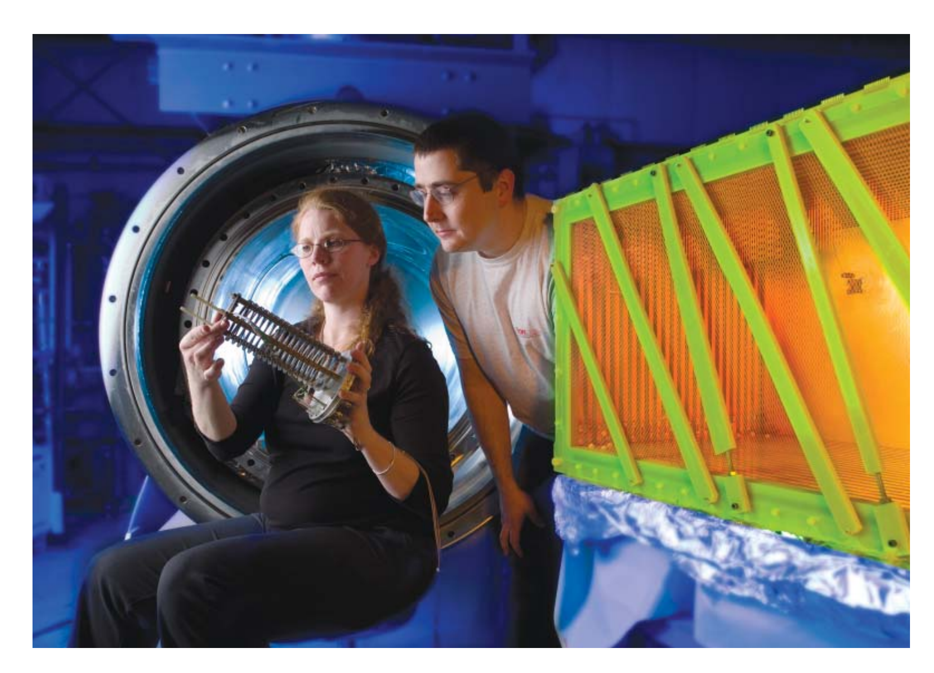
El año pasado, los investigadores que participaron en el estudio MiniBooNE, concebido para la detección de unas escurridizas partículas subatómicas llamadas neutrinos, anunciaron una anomalía sorprendente. Los neutrinos, partículas desprovistas de carga y con una masa muy pequeña, se forman a partir de reacciones nucleares y en desintegraciones de partículas subatómicas. Hay tres tipos, o sabores, de neutrinos: neutrinos de electrón, de muon y de tauon; a lo largo de su camino, los neutrinos van oscilando de unos de esos tipos a los otros.

Los investigadores de MiniBooNE, mientras observaban un haz de neutrinos muónicos generados en uno de los aceleradores del Fermilab, se encontraron con que un número inusitadamente grande de las partículas pertenecientes a las más bajas energías (inferiores a 475 millones de electronvolt) se había convertido en neutrinos electrónicos. Después de un año de diferentes análisis, les ha sido imposible dar con una explicación corriente de lo que han dado en llamar "exceso a baja energía". El misterio ha hecho recaer la atención sobre una hipótesis llamativa: la existencia de una cuarta categoría de neutrinos que se muevan desde y hacia otras dimensiones.

La teoría de cuerdas, que se propone unificar las leyes de la gravitación y la mecánica cuántica, había pronosticado hace bastantes años la existencia de dimensiones adicionales. Algunos físicos han propuesto que casi todas las partículas de nuestro universo pudieran hallarse confinadas en un subespacio tetradimensional incrustado en un espacio de diez dimensiones; el primero sería una "brana" (de "mem*brana*"), el otro, el grueso del espacio ("bulk"). Postulan, además, la existencia de una partícula, a la que denominan "neutrino estéril", que solamente interactúa con las partículas no neutrínicas por mediación de la gravedad, y que entraría o saldría del espacio de cuatro dimensiones y tomaría atajos a través de las demás. En 2005, Heinrich Päs, de la Universidad de Dortmund, Sandip Pakvasa, de la de Hawai, y Thomas J. Weiler, de Vanderbilt, pronosticaron que las peregrinaciones supradimensionales de los neutrinos estériles incrementarían la probabilidad de oscilaciones entre sabores en energías bajas. Eso fue precisamente lo observado en MiniBooNE dos años después.

Muy alentado por la perspectiva de descubrir nuevas leyes de la física, el equipo de MiniBooNE ha propuesto una segunda parte de su experimento a la que denominan MicroBooNE; tal vez permita verificar la hipótesis del neutrino estéril. Un detector nuevo, basado en un tanque criogénico con 170 toneladas de argón líquido, detectaría partículas de bajas energías con precisión mucho mayor que su antecesor. Las partículas emergentes de una interacción con neutrinos ionizarían átomos de argón que se hallasen en su trayectoria, y estos iones inducirían corrientes eléctricas en matrices de hilos conductores instaladas en la periferia del tanque. Con los datos obtenidos podría establecerse con precisión la trayectoria de la partícula, diferenciar mejor las interacciones de neutrinos electrónicos de otros fenómenos y, finalmente, determinar si existe un auténtico exceso de oscilaciones de sabor a bajas energías.

El tanque de MicroBooNE, que costaría unos 15 millones de euros, se ubicaría en las proximidades del detector MiniBooNE del Fermilab, para que observara el mismo haz de neutrinos. La comisión de físicos asesores del laboratorio aprobó en junio pasado la fase de diseño del proyecto, y si todo va bien, el detector comenzará a funcionar ya en 2011. Se confía en que MicroBooNE dé paso al desarrollo de detectores mucho mayores, con cientos de toneladas de argón líquido, del tamaño de campos de deportes. Tales instalaciones permitirían investigar otros fenómenos conjeturados, como la desintegración de los protones, que es extraordinariamente rara.



FERMILAB

Dos cazadores de neutrinos, Bonnie Fleming y Mitchell Soderberg, inspeccionan un prototipo de detector basado en argón líquido, llamado ArgoNeuT, primer paso hacia el experimento MicroBooNE, del Fermilab.

Mark Alpert

EL DERECHO A ESTAR SOLO

Se están desplazando las lindes entre el interés público y el derecho a la intimidad

Peter Brown

Vientos gélidos barren la privacidad. Los avances técnicos y el contraterrorismo provocan cambios impresionantes, tal vez irreversibles, en lo que cabe esperar que subsista de vida privada. Hace unos diez años, Scott McNealy, de Sun Microsystems, predijo la muerte de la privacidad. "Pechad con ello", fue su consejo. Hay quienes, sobre todo jóvenes menores de 25 años, se jactan de haber seguido la recomendación estrictamente. Han abrazado la antítesis de lo privado: la apertura total a la mirada pública. Y, desde luego, en muchos casos, como la detección de terroristas o la de portadores de ciertas enfermedades, el interés público cuenta con buenas razones para recabar información sobre materias que normalmente pertenecerían al ámbito privado.

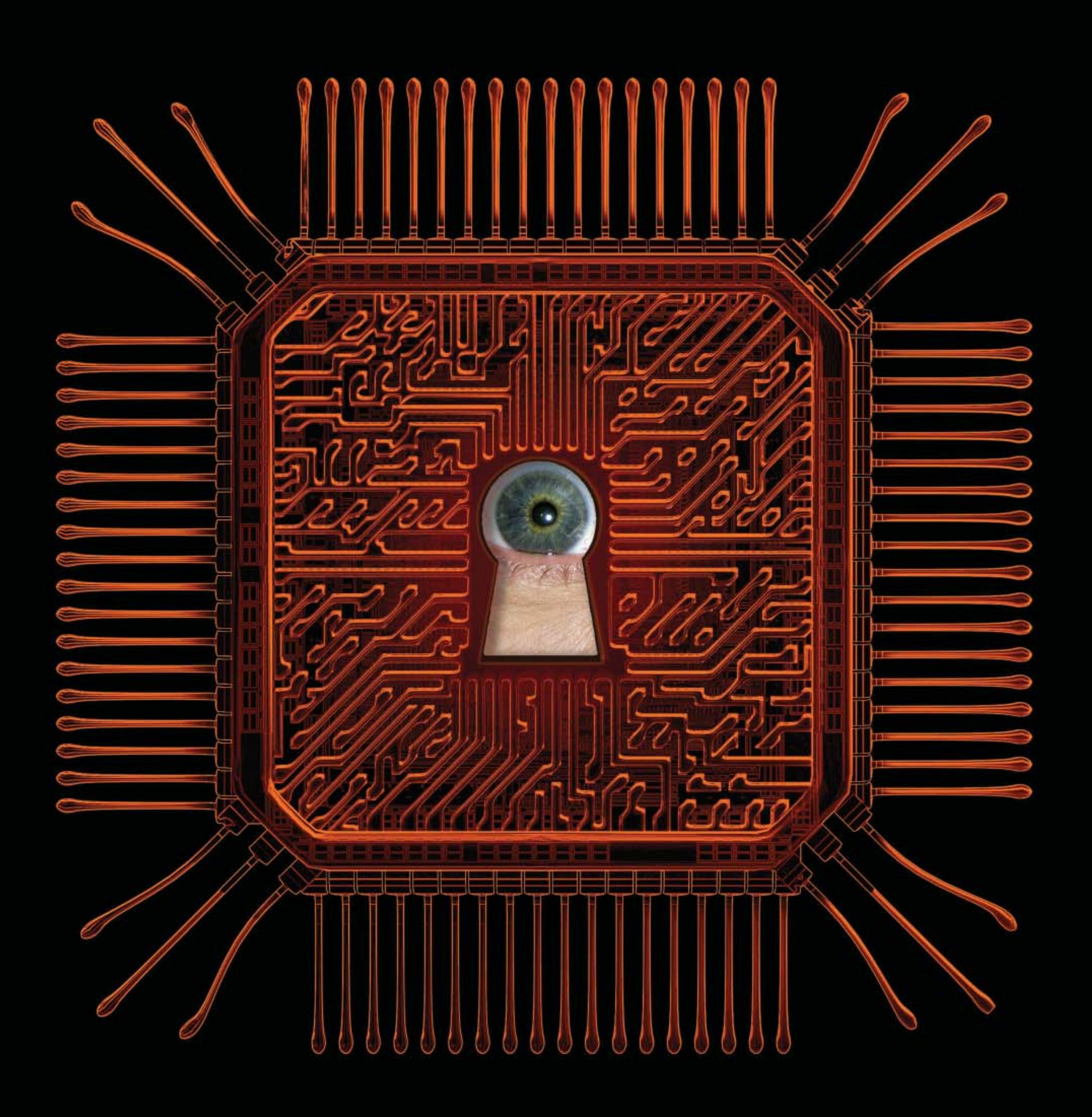
Por otra parte, hay contextos —en la banca o en el comercio, en la diplomacia o la medicina— donde la privacidad de las comunicaciones resulta esencial. Los fundadores de Estados Unidos de América pusieron gran énfasis en el respeto a la esfera privada, y lo sustanciaron en la Declaración de Derechos (si bien, como a menudo se nos recuerda, sin explicitarlo). Esther Dyson, en el ensayo que abre este monográfico, deslinda el significado de "privacidad" al recordarnos en qué no consiste: diversas e importantes cuestiones, que con frecuencia se presentan ligadas a la noción de privacidad, quedan mucho más claras enfocadas como asuntos relativos a la seguridad personal o colectiva, a la política sanitaria, a las relaciones con las compañías de seguros o al derecho a la propia imagen.

El terrorismo y la conectividad informática confieren a la privacidad una gran carga emotiva y política, pero existe una multitud de otros, y excelentes, motivos para examinar de cerca su futuro.

Un segundo motivo son los seductores beneficios que se seguirían de la disponibilidad de cierta clase de informaciones: servicios médicos más perfectos por la informatización de historiales médicos o genéticos, o una protección más completa frente a suplantaciones de identidad lograda mediante sistemas de autorización biométrica. Un tercer motivo es que las amenazas que la técnica le plantea a la privacidad, e incluso a la seguridad de las personas, no tienen precedentes, en cuanto a efectos no buscados, consecuencia de las informaciones más completas que sobre sí mismos facilitan los propios individuos, y en cuanto a la veloz evolución y perfeccionamiento de los dispositivos de vigilancia, de los chips de identificación por radiofrecuencia o de la fusión de datos, por no mencionar los virus y demás plagas que infestan Internet.

Ante todas estas amenazas contra la privacidad, se ha ideado una pasmosa variedad de sistemas técnicos destinados a protegerla, a los que, sin embargo, apenas se recurre. Tal vez ello se deba, en parte, a que muchos jóvenes consideran que estas angustias por la privacidad son humo de pajas. Muchos, en la nueva generación, están encantados de trocar la idea de "información privada" de sus progenitores por una vida rica en la pecera transparente de las redes sociales.

Por todas estas razones y otras muchas, se dedica este número al futuro de aquello que Louis D. Brandeis, del Tribunal Supremo estadounidense, dio en llamar "el derecho a estar solo".





REFLEXIONES SOBRE LA NUEVA PRIVACIDAD

Cuestiones que en apariencia conciernen a la intimidad personal consisten en realidad en problemas de seguridad, de política sanitaria, de aseguración o de imagen personal

Esther Dyson

CONCEPTOS BASICOS

- En muchos casos, las presuntas erosiones de la privacidad se encuadran mejor en perjuicios de otras clases.
- Las "pérdidas de privacidad" pueden consistir realmente en mermas de seguridad.
- Muchos de los temores en Estados Unidos que conciernen a la privacidad genética (aunque no todos) desaparecerían si la atención médica estuviese allí al alcance de todos.
- Los ciudadanos han de tener derecho a supervisar las actividades del gobierno y de sus funcionarios, y a darlas a conocer en la Red.
- Estamos empezando a disponer de medios eficaces para controlar la información personal que queremos revelar y a quiénes se les facilita.

La privacidad es un test de Rorschach público: menciónesela, y al momento asistiremos a encendidas disquisiciones. A unos les preocupan los abusos de poder del gobierno; otros temen que sea conocido su pasado con las drogas o su conducta sexual; los hay que se despachan contra las empresas, que se apropian de datos personales para mejor orientar su publicidad, o contra las indagaciones de las aseguradoras acerca de la historia médica de sus solicitantes. Se teme un mundo de comercialización invasora, donde los datos encasillarían a los individuos en determinados "segmentos de consumo", perfectamente ajustados a sus deseos más íntimos o a sus caprichos más frívolos. Y no faltan quienes tiemblen ante las intromisiones del gobierno o las imposiciones sociales.

Cuando se habla de estos temores, se suele considerarlos parte de un tira y afloja: entre privacidad y atención sanitaria efectiva; privacidad y uso libre y gratuito de creaciones de un tipo o de otro (en sitios costeados por la publicidad); privacidad y seguridad personal o colectiva. Debates todos ellos muy manidos, ahora otra vez en primer plano, pero de muy distinto modo al de los tiempos en que sólo interesaban a especialistas, círculos restringidos o tenaces defensores de su intimidad personal.

Por una parte, la erosión que sufre la privacidad es innegable. Somos muchos quienes operamos en la Red y probablemente casi todos nos hemos preguntado con sorpresa más de una vez: "¿Cómo se sabe eso de mí?" La Administración estadounidense está invadiendo por todos lados la intimidad de las personas y llevando a cabo más y más operaciones en la oscuridad. Cada vez resulta más difícil actuar de forma anónima si alguien —y en especial si ese alguien es el gobierno— desea averiguar quién lo está haciendo.

Y por otro lado, han surgido razones nuevas y poderosas para que los individuos revelen información privada. La medicina personalizada está a punto de convertirse en realidad. Son enormes las posibilidades que para mejorar el bienestar general ofrece la posesión de información detallada y exacta de carácter sanitario y genético, información que ha de ser extraída de historias clínicas de particulares, y que es útil por igual para el tratamiento de individuos como para análisis estadísticos o epidemiológicos de poblaciones. Muchas personas disfrutan compartiendo en Internet informaciones de índole muy personal en las



1. UNO DE LOS EFECTOS DE INTERNET es la dilución de fronteras entre individuos, límites antaño tradicionales en nuestra sociedad. Este fenómeno nos obligará a afrontar cuestiones éticas que no hubieran surgido cuando la información se encontraba compartimentada. Así nos lo hacen ver los personajes ficticios de la fotografía. Si se tratase de casos genuinos y fuesen colgados en la Red, se plantearían espinosos problemas éticos.

MARK CLEMENS (*Fotoilustración*); RICHARD NOWITZ *National Geographic Collection* (*muchedumbre*)

llamadas redes sociales. En un plano más turbio, la insistencia en la amenaza terrorista ha llevado a muchos a ceder información privada a cambio de ilusorias promesas de seguridad personal o colectiva.

Gran parte del respeto a la intimidad tenido por evidente en otros tiempos ha sido un subproducto de la fricción consiguiente a la búsqueda y ensamblaje de información sobre las personas. Esa fricción ha desaparecido casi totalmente. Todos vivimos hoy como los famosos: nuestros movimientos son observables, nuestros aumentos de peso o los días en que nos hemos levantado con mal pie, motivo de comentarios. Preguntas antes que tenidas por indiscretas son explícitas hoy: "Ese con quien cenabas, ¿era un ligue?" o "De tus amigos, ¿cuál es el mejor?"

Condiciones de contorno

Este número de Investigación y Ciencia se ocupa de las técnicas que degradan nuestra intimidad y las que contribuyen a preservarla. Para mejor encuadrar la exposición, séame permitido establecer tres puntos de referencia.

Primero, para establecer que la cesión de una determinada información constituye una invasión de nuestra privacidad, resulta útil distinguir los posibles perjuicios objetivos consecuentes a tal revelación —sufrir un fraude, denegar un servicio o ser privados de libertad— de cualesquiera otros de carácter subjetivo, en los cuales lo tenido por lesivo es el mero conocimiento por una segunda o tercera persona de información que nos concierne. En muchos casos, la presunta invasión de privacidad constituye en realidad una merma de nuestra seguridad o un perjuicio económico: si los datos que me identifican, o los de mis tarjetas de crédito, son conocidos por terceros y utilizados indebidamente —y es probable que facilitemos esos datos varias veces al mes—, no es mi intimidad la que sufre, sino mi seguridad o mi cuenta corriente. En cuanto a las invasiones de la privacidad propiamente dicha, los "perjuicios" que cada cual percibe son subjetivos e individuales. Por eso, en lugar buscar una definición de privacidad de validez universal, la sociedad debería facilitar a los individuos los medios para controlar el uso y difusión de sus datos. El equilibrio entre lo secreto y lo revelado es una cuestión de preferencia individual, pero la necesidad de instrumentos, e incluso de leyes, que faculten para ejercer esas preferencias es de carácter general.

Segundo, mientras se dibujan las nuevas lindes entre lo público y lo privado, el público ha de conservar el derecho a dar testimonio o a denunciar. Siendo el terreno de lo estrictamente personal cada vez más reducido, para preservar la libertad y equilibrar los intereses

La autora

Esther Dyson es inversora en nuevas empresas, entre ellas 23andMe (análisis del genoma a petición propia), PatientsLikeMe (información médica compartida en línea) and Boxbe (preferencias de correo electrónico dirigidas por los usuarios). Dyson y otras nueve personas se disponen a publicar "en línea" sus secuencias genómicas completas, acompañadas de información sobre su salud, dentro del Proyecto Genoma Personal. Dyson señala: "Estuve recientemente estudiando el mercado de los seguros médicos. Le pregunté a mi agente si deseaba tener una copia de mi genoma, y la rechazó cortésmente". Dyson es autora de *Release 2.0*, un libro que se ocupaba de la privacidad en la Red ya en 1997.

de los individuos y los de las instituciones en un mundo de datos que se pueden rastrear sin tropiezos, resulta fundamental que los individuos tengan, a su vez, derecho a rastrear y dar a conocer las actividades de organizaciones poderosas, trátese de gobiernos o de grandes empresas.

El tercer punto es desarrollo del primero: en la valoración de los cambios en las expectativas sobre la privacidad, se ha de tener en cuenta que el control de cada uno sobre sus datos presenta un carácter "granular". La privacidad no viene en talla única: personas diferentes muestran en distintos momentos preferencias diversas sobre lo que le pueda ocurrir a información personal suya y sobre quiénes tienen acceso a ella. Tal vez no posean el derecho, o no cuenten con la capacidad necesaria, para imponer sus condiciones en relaciones coercitivas —por ejemplo, con un organismo gubernativo— o al tratar con quienes deseamos que nos proporcionen algo a cambio, como un empresario o una compañía de seguros. Pero a menudo se tiene mejor posición para regatear de lo que se cree. Y ahora estamos adquiriendo los medios y conocimientos necesarios para sacar provecho de tal posición.

Perjuicios objetivos

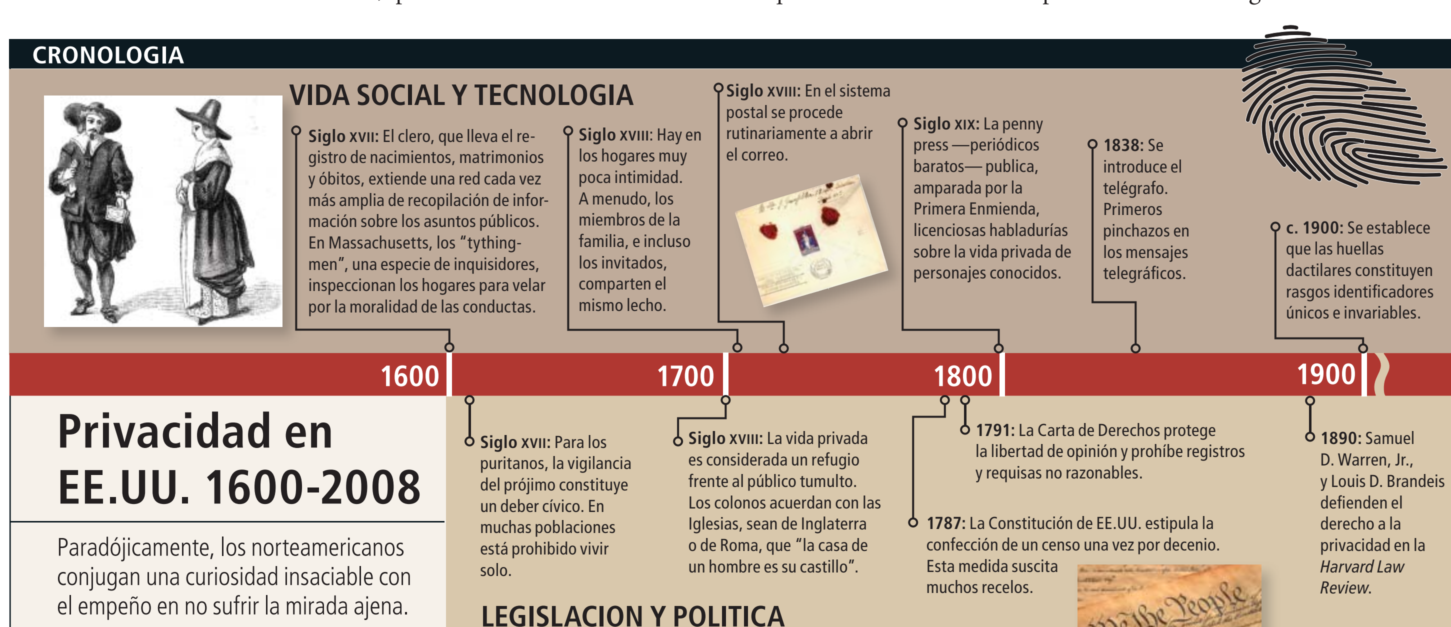
No es la seguridad el único asunto de interés público que es presentado como una cuestión de privacidad. Muchos aspectos de la privacidad médica o genética, por ejemplo, constituyen en realidad asuntos dinerarios o de relaciones con las entidades aseguradoras. ¿Deben las personas de salud delicada verse obligadas a pagar primas más elevadas por los servicios médicos? Si usted considera que no, podría sentirse llevado a concluir que a tales personas debería tácitamente permitírseles que mintieran. Esta conclusión es, a menudo y erróneamente, encuadrada en la protección de la intimidad. La verdadera cuestión, empero, no es la privacidad, sino el modelo de negocio de los seguros médicos. A la gente no le importaría tanto que se conociera toda la verdad sobre su salud si ello no les expusiera a costosos honorarios médicos y a recargos en las primas de los seguros.

Los datos genéticos parecen ofrecer un ejemplo especialmente inquietante de posibles discriminaciones. Uno de los temores es que, a no tardar, las compañías de seguros les exijan a los solicitantes que se sometan a exámenes genéticos y nieguen cobertura a quienes arrojen determinados resultados. El genoma es portador, no cabe duda, de una importante cantidad de información. Puede identificar unívocamente a cada persona, salvo los gemelos idénticos. Puede también revelar relaciones familiares que pudieran hallarse ocultas. Ciertas enfermedades raras son diagnosticables por la presencia de ciertos marcadores genéticos.

Pero los genes constituyen sólo uno de los ingredientes de la vida de las personas. Poco podrán contarnos sobre la dinámica familiar o decir qué uso ha dado esa persona a sus facultades innatas. La manifestación de los genes depende de complejas interacciones con la crianza y educación del individuo, con su conducta, con el ambiente en el que vive y, por supuesto, con el azar.

Y es muy posible que la discriminación genética sea muy pronto prohibida por las leyes. En mayo de 2008, el presidente George W. Bush firmó y convirtió en ley la no discriminación por información genética

FUENTE DE LA LINEA TEMPORAL: *BEN FRANKLIN'S WEB SITE*, POR ROBERT ELLIS SMITH. PRIVACY JOURNAL, 2000 (WWW.PRIVACYJOURNAL.NET); MPI/GETTY IMAGES (*Puritanos*); IMAGEZOO/IMAGES.COM/CORBIS (*sobre*); TODD GIPSTEIN *Corbis* (*Preámbulo de la Constitución de los EE.UU.*)



(GINA, Genetic Information Nondiscrimination Act), que ilegaliza toda discriminación en seguros o empleos que se base en tests genéticos.

No obstante, es muy probable que la riada de información médica y genética que está al llegar altere la naturaleza misma de los seguros médicos. Gracias a la existencia de mayores flujos de información concernientes a grupos muy amplios, obtenidos merced a seguimientos más completos de las enfermedades y los resultados de sus tratamientos, resulta cada vez más sencillo efectuar pronósticos precisos fundados en estudios estadísticos.

Pero si los individuos van a poder ser asignados a las llamadas "cestas de costes" con razonable precisión, el aseguramiento contra gastos médicos elevados deja de ser una cuestión de valoración comunitaria, de agregación de recursos de un grupo para afrontar riesgos individuales desconocidos. Se trata, por el contrario, de imponer a la sociedad en su conjunto el pago de subsidios para proporcionar seguros a precios razonables a aquellas personas que, por su elevado riesgo de enfermar, tendrían que afrontar primas o tratamientos médicos de coste prohibitivo.

En consecuencia, la sociedad tendrá que decidir, clara y abiertamente, qué clases de discriminación son aceptables y cuáles no. Todos nos veremos obligados a plantearnos con nitidez las opciones éticas, en lugar de ocultarnos en la confusión y en la opacidad de información. Si a las aseguradoras se les pide que administren subsidios, exigirán reglas claras sobre los costes sanitarios individuales y qué tanto por ciento de ellos desea la sociedad que se proporcionen y está dispuesta a pagar. (La solución consiste, como siempre, en lograr que aseguradoras y servicios de salud rebajen los costes y sigan prestando buena atención y cuidados a sus asegurados, en lugar de limitar los servicios. Una información más completa sobre los riesgos sanitarios y los resultados de los tratamientos, como ya he mencionado arriba, contribuirá a medir la eficacia del servicio y a controlar mejor los gastos.)

DILEMAS DE LAS PRUEBAS DE IDENTIDAD

A menudo tenemos que demostrar quiénes somos; por ejemplo, para pedir trabajo, conducir, o solicitar un crédito.

Pero es tanta la información disponible sobre las personas, que resulta relativamente fácil suplantar la personalidad de alguien.

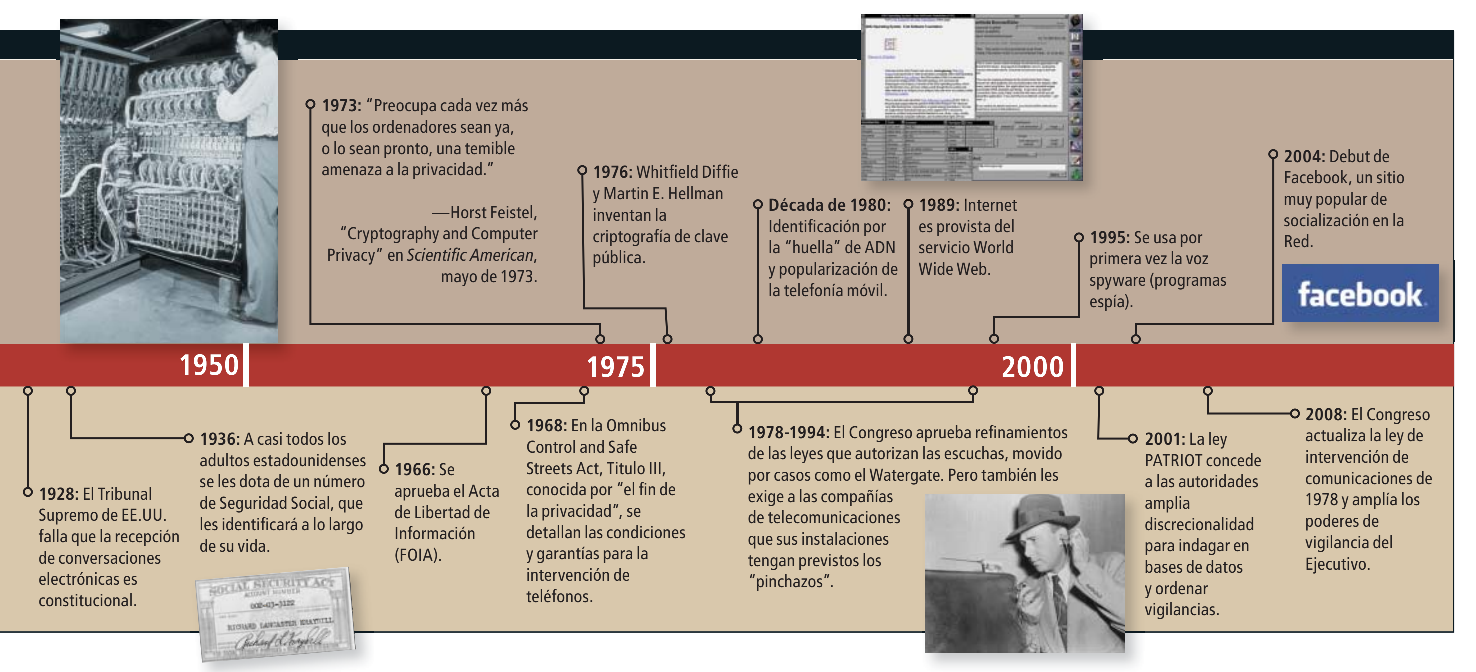
Y en el ínterin, ¿qué ha de hacer la sociedad con quienes no puedan o no deseen demostrar quiénes son? ¿Qué hacer con inmigrantes indocumentados, con quienes desean empezar de nuevo o quienes, sencillamente, quieren permanecer anónimos?

El derecho a prestar testimonio

Las normas sobre privacidad son necesarias cuando una de las partes tiene la potestad de exigirle datos a la otra. El ejemplo más importante nos lo ofrece el poder del gobierno para recoger y usar (o abusar de) datos personales. Debe ponerse coto a ese poder.

¿Cuál es la mejor forma de limitar el poder del gobierno? No mediante normas que protejan la intimidad de los individuos, que el gobierno puede dejar de obedecer, o de hacer obedecer, sino mediante normas que limiten la privacidad del gobierno y de los funcionarios. El público ha de conservar el derecho a saber y el derecho a dar testimonio.

Los medios de comunicación han constituido tradicionalmente un instrumento primordial para ejercer ese derecho. Pero Internet le está proporcionando a la gente las herramientas y la plataforma para tomar tales asuntos en sus manos. Cada cámara fotográfica o grabadora de vídeo puede servir para dar público testimonio de actos de opresión, como ya demostró en 1991 el vídeo de Rodney King, y como lo han probado las fotografías de la prisión de Abu Ghraib en 2004. Internet es la plataforma que les proporciona a todos acceso instantáneo a un público que es, en teoría, el mundo entero. Los informes de las ONG y de ciudadanos particulares de todo



ARCHIVE HOLDINGS, INC (*técnico informático*); BETTMANN/CORBIS (*tarjeta de la Seguridad Social y hombre con dispositivo de escucha*); GÜRKAN SENGÜN *http://livecd.gnustep.org (página web)*; FACEBOOK (*logo*)





2. LAS VENTAJAS E INCONVENIENTES del acceso a los archivos electrónicos de datos personales se aprecian con claridad en el dilema de las historias clínicas. Estos datos podrían salvarle la vida a un accidentado inconsciente (*izquierda*), pero si revelasen problemas de salud muy onerosos, las aseguradoras podrían negarle la cobertura médica (*arriba*).



UNA VIA DE DOBLE SENTIDO

El derecho a dar testimonio, a rastrear las actividades del gobierno e informar sobre ellas, de igual forma que el gobierno recopila información sobre nosotros, es crucial para preservar la libertad.

Históricamente, los ciudadanos estadounidenses han podido estar al tanto de los actos del gobierno por:

- **Los medios de comunicación**
- **Las actas del Congreso**
- **Otros documentos públicos**
- **Leyes como la FOIA (de libertad de información)**

Internet ofrece ahora nuevas vías de supervisión y denuncia de:

- **Actividades de funcionarios públicos**
- **Conflictos de interés**
- **Seguimiento de los datos que se entregan al gobierno**
- **La protección y seguridad de esos datos**

el mundo se distribuyen por Internet gracias a las redes sociales y a los sitios de archivos compartidos, así como mediante mensajes de texto por teléfono móvil.

Resulta un tanto irónico que el mejor modelo de lo que los ciudadanos han de exigir a sus gobiernos sea, posiblemente, el tipo de información que los gobiernos les exigen a las empresas. Las normas de transparencia para las actividades empresariales son cada vez más estrictas: sus prácticas laborales, los resultados económicos, en una palabra todo cuanto se hace en la empresa. Los socios o accionistas tienen derecho a conocer cuanto concierne a la compañía que poseen y los clientes tienen derecho a informarse sobre los ingredientes de los productos que compran y sobre su proceso de producción.

Por la misma regla, los ciudadanos tenemos derecho a conocer aquellas conductas de las personas a quienes elegimos y mantenemos en lo que concierna a los cargos que desempeñan. Tenemos el derecho a conocer sus conflictos de intereses: a saber, a qué dedican su tiempo (¡nuestro tiempo!) los funcionarios públicos. Ante el gobierno, debemos gozar de los mismos derechos que los accionistas o los consumidores con respecto a las empresas, o si se prefiere, los que posee la U.S. Securities and Exchange Commission (aproximadamente equivalente a la Comisión Nacional del Mercado de Valores) con respecto a las compañías que cotizan públicamente.

De hecho, me atrevo a sostener, los ciudadanos poseen con respecto al gobierno derechos aún mayores, precisamente porque se ven obligados a facilitarle tantísima información de carácter personal. Tendríamos que poder supervisar qué hace el gobierno con nuestros datos personales y auditar (por medio de representantes) los procesos de manejo de los datos y de su protección y seguridad. La Fundación Sunlight (www.sunlightfoundation.com), a cuyo consejo de administración pertenezco, está animando a la gente a averiguar y publicar en la Red información concerniente a sus diputados en el Congreso y, en definitiva, sobre todos los funcionarios públicos.

Empresas a plena luz

En cuanto a los derechos de privacidad de las empresas, ni tienen muchos, ni deben tenerlos. Es cierto que tienen derecho a archivar sus transacciones con los clientes y que, por lo general, las transacciones a crédito requieren que los clientes demuestren su fiabilidad aportando información adecuada. Pero exactamente lo mismo que una compañía puede negarse a vender a crédito, el cliente puede negarse a negociar con las compañías que le exijan demasiados datos. Aparte de eso, todo debería ser negociable. Los clientes pueden exigir saber lo que las compañías hacen con sus datos y, si la respuesta no les satisface, tratar con otras. Lo que la ley ha de garantizar es que las empresas se atengan realmente a las reglas que dicen seguir.

Como ocurre con las revelaciones por el gobierno (y en especial, por los políticos cuando buscan cargos), las revelaciones sobre negocios están yendo más allá de lo exigido por la normativa. En todas las esferas de actividad, el

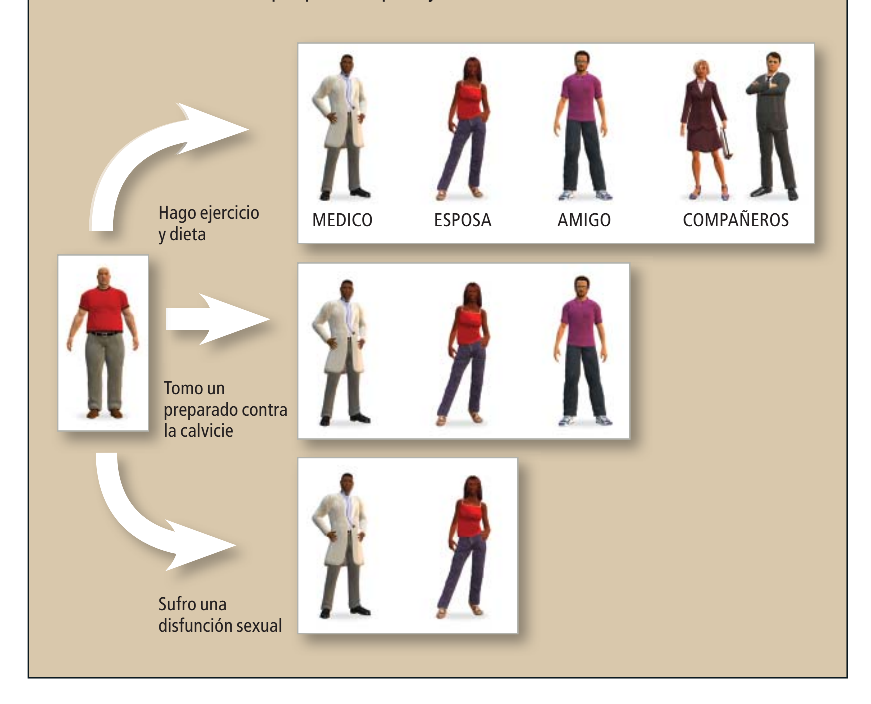
COMSTOCK/CORBIS (*ambulancia*); RANDY FARIS *Corbis (foto de archivo)*; LARRY DOWNING *Sygma/Corbis (sello presidencial)*

individuo común no se calla. Hay todo tipo de sitios en la Red dedicados a valoraciones, debates y otros contenidos, generados por los usuarios, sobre productos y servicios: hoteles, médicos y similares. Desde luego, muchas de las críticas de hoteles que aparecen en esos sitios las escriben los propios hoteles o sus competidores. (Para frenar tales tácticas, algunos sitios solicitan biografías de los usuarios y animan, a su vez, a los usuarios a valorar la credibilidad de otros usuarios o comentaristas.) Los enfermos pueden valorar a médicos y hospitales en una variedad de sitios, desde HealthGrades.com (un servicio de pago) hasta cierto número de sitios que se mantienen por la publicidad.

Al respecto de información sobre productos materiales proporcionada por usuarios, consideremos una nuevo servicio, Barcode Wikipedia (www.sicamp.org/?page-id=21), la wikipedia del código de barras. Este servicio permitirá a los usuarios colocar en la Red lo que sepan o puedan averiguar sobre un producto: sus ingredientes o componentes, si ha sido manufacturado o meramente ensamblado, las prácticas laborales del fabricante o sus efectos medioambientales. Las compañías tienen también libertad para publicar en esa página y exponer su versión. Con un acceso tan amplio, cabe esperar que los informes abunden en exageraciones, falsedades e información útil. No obstante, con el tiempo, como la propia Wikipedia ha demostrado, los usuarios velarán unos por otros y la verdad, más o menos aproximada, acabará por aflorar.

Revelación gradual

Es muy posible que un hombre grueso y calvo quiera controlar qué porciones de su historial médico electrónico son conocidas por distintos grupos de personas. Su calvicie y su volumen resultan obvios (aunque no facilite su peso con precisión), pero no ve la necesidad de que su participación en el plan de dieta y ejercicio de su empleador trascienda de su médico, su mujer y sus amigos o colegas. Accederá a que el médico y sus íntimos sepan que toma un medicamento contra la calvicie, pero no a que su disfunción sexual sea conocida, excepto por su esposa y su médico.



KENN BROWN *Mondolithic Studios*

Vivir en público

Hasta hace poco tiempo, para la mayoría de la gente la privacidad venía dada (aunque no garantizada) por las dificultades con que tropezaba la obtención de información. Por otra parte, la información sobre lo que cada cual hacía en privado no llegaba demasiado lejos, a menos que se tratase de alguien famoso o se tomase muchas molestias por hacer públicas sus actividades. Pero ahora el concepto mismo de privacidad está cambiando. Muchos adultos se quedan boquiabiertos ante lo que se puede encontrar en Facebook o MySpace. Algunos adolescentes son conscientes de los peligros de utilizar redes de socialización en la Red, pero no se los toman en serio: tal es una de las inmemoriales limitaciones de la adolescencia. Y es verosímil que llegue a tomar cuerpo algún tipo de período de prescripción para las conductas alocadas. La mayoría de los empleadores (que pueden examinar en la Red las páginas de los solicitantes de empleos lo mismo que cualquiera) se limitarán a aplicar criterios más laxos y seguirán dando empleo, pero otros pueden mostrarse más estrictos. Tomemos, por ejemplo, los tatuajes. Hace 20 años, los adultos los prohibían o advertían a los adolescentes en su contra. Ahora, en el vestuario del club deportivo que frecuento, la mitad de las mujeres están tatuadas y presumo que entre los hombres será válida una proporción igual o mayor.

Los adolescentes conservan todavía un sentimiento de intimidad y siguen hiriéndoles las opiniones de otros. Se han habituado, más que sus padres, a pasar en público una parte mucho mayor de sus vidas. Se trata, a mi parecer, de un auténtico cambio. No se olvide, sin embargo, que el siglo XX señaló también un gran cambio con respecto al XIX en cuanto a la privacidad. En el siglo XIX eran pocas las personas que dormían solas: los niños lo hacían juntos en un mismo cuarto o compartían el dormitorio con sus padres. Los ricos tenían sus habitaciones propias, pero también criados para retirar sus orinales, para ayudarles a vestirse o para atender a sus necesidades más íntimas. Nuestras nociones de intimidad física, que se han ido forjando durante el siglo XX, son francamente nuevas.

Durante siglos, en los pueblos casi todo el mundo sabía muchísimo de los demás. Aunque era poco lo que se explicitaba. Mas en el pasado, y ahí radica la diferencia real, Juan no podía conectarse a la Red y ver y oír lo que estaba diciendo Ana. Juan podría haber conjeturado lo que Ana sabía, pero podía darse por no enterado de lo que Ana supiera. De igual modo, Juan podía fácilmente evitar tropezarse con Ana. En nuestros días, si Juan es la ex pareja de Ana, es muy libre de atormentarse viéndola flirtear en la Red. ¿Podrá existir una noción de intimidad frente a los propios deseos?

Mis datos, mi yo

Un segundo y gran cambio en el problema de la intimidad personal es que se está aprendiendo a ejercer cierto control sobre qué datos pueden ver los demás. Facebook les ha proporcionado a millones de personas instrumentos para ello y, de forma un tanto involuntaria, la práctica en utilizarlos. El año pasado, Facebook molestó a algunos de sus usuarios con un servicio llamado Beacon, que rastreaba sus compras efectuadas en otros sitios de la Red y las daba a conocer a sus amigos. Aunque se había informado de tal práctica, no se realizó de modo eficaz; en consecuencia, muchos usuarios utilizaron los controles de privacidad que previamente habían pasado por alto. (Facebook, posteriormente, reajustó las cosas dándoles un enfoque más sensato y el revuelo se apaciguó.) Ahora, son muchos los miembros de Facebook que han cambiado sus controles de privacidad, tanto para recibir noticias de sus amigos (¿de verdad quieres enterarte de cada vez que Manuel sale con alguien?) como para comunicarles noticias sobre sí mismos (¿de verdad quieres contar a todos cómo te ha ido en tu último viaje profesional?). Los usuarios pueden compartir fotografías con grupos privados y colgarlas abiertamente, para que las vea quien lo desee.

Flickr, un sitio de la Red para compartir fotografías, ofrece a los usuarios cierto grado de control sobre quiénes pueden verlas, aunque no absoluto (debo advertir de que soy inversora en Flickr). Es probable que estos controles se hagan más precisos. En la actualidad podemos, si se desea, definir un grupo cerrado, lo que no es exactamente igual que poder hacer revelaciones selectivas a amigos concretos. Imaginemos, por ejemplo, que deseamos crear dos grupos familiares que se superponen en parte. Uno de ellos podría estar compuesto por nuestros hermanos hijos de nuestra madre y nuestro padre, y el otro, por todos los hermanos y hermanastros, nuestra madrastra y nuestro padre, pero excluyendo a nuestra madre. Otras personas podrían crear otros subconjuntos familiares —un padre y sus hijos, por ejemplo, pero no su nueva esposa— cuya mera existencia podría ser necesario mantener discretamente en el estricto ámbito familiar.

La autora de blogs y experta en redes sociales danah boyd (así, en minúsculas), miembro no residente del Centro Berkman para Internet y Sociedad de la Universidad de Harvard, disertó elocuentemente hace poco sobre el deseo de los usuarios de controlar exactamente quiénes verán lo que cuelguen en la Red y qué anuncios lo acompañarán. Dicho de otro modo, lo que importa no son los anuncios que yo veo, sino los que mis amigos ven en "mi" página de la Red. Para boyd —y muchos otros— lo que importa no es tanto la privacidad cuanto la presentación que la persona hace de sí misma (que en el caso de boyd incluye la grafía de su nombre).

Todo el mundo es consciente de que no puede controlar lo que a su respecto digan los demás, pero la gente saldrá de estampida hacia servicios comunitarios en línea que les permitan controlar la forma de presentarse ante los demás y quiénes pueden ver determinadas presentaciones. Esa clase de control se extenderá, según creo, a los vendedores que aprovechen las redes de amistades creadas en las redes sociales de Internet. A Ana puede parecerle bien que la tienda que le vendió un suéter rojo de talla masculina conozca sus hábitos de compra, pero quizá no quiera que sus amigas, su pareja actual u otros vendedores accedan a esa información. Evidentemente, Ana no puede controlar lo que otras personas sepan o digan de ella. Pero si Juan, su ex pareja, sigue poniéndose el suéter rojo después de que rompieran, alguien podría darse cuenta. Y combinar esa información de mil maneras.

No obstante, la transparencia no simplifica las cosas. Estos nuevos instrumentos sociales hacen que las cosas, las vidas y las relaciones parezcan ser exactamente todo lo complejas que son o tal vez todo lo complicadas que alguien esté dispuesto a revelar. No existe una única verdad, ni una lista sencilla de a quiénes se les permite saber según qué cosas. La ambigüedad es una constante en la historia y en la literatura, en las campañas políticas y en las negociaciones de contratos, en el lanzamiento de nuevos productos, en las cartas de agradecimiento y en las formas de cortesía, por no mencionar divorcios, querellas judiciales, dimisiones de empleados o invitaciones para comer ofrecidas sin ganas. La ambigüedad no va a desaparecer porque se sazone con informática.

Bibliografía complementaria

PRIVACY 2.0: A DESIGN FOR LIVING IN THE DIGITAL AGE. Esther Dyson. Broadway Books, 1997.

SITIO EN LA RED DE BEN FRANKLIN: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET. Robert Ellis Smith. Privacy Journal, 2000. www.privacyjournal.net

Acerca de las reflexiones de Esther Dyson sobre cesión de datos y transparencia visite, www.huffingtonpost.com/esther-dyson

Existe más información sobre el Proyecto Genoma Personal en www.personalgenomes.org

Para informarse sobre la Sunlight Foundation y sus instrumentos para lograr transparencia, visite www.sunlightfoundation.com



ESPIONAJE EN LA RED

Trasladadas a Internet las conversaciones telefónicas, allá se han mudado también quienes desean intervenirlas. Las técnicas necesarias entrañan una peligrosa ampliación de la capacidad de vigilar de los gobiernos

Whitfield Diffie y Susan Landau

Donde se haya conversado en privado, siempre habrá habido quien a hurtadillas lo escuchase. La voz inglesa para quienes así fisgonean —*eavesdroppers*— alude a los entrometidos que se ocultaban bajo el alero (*eaves*), o bajo las gotas (*drops*) que caían del alero, para escuchar. Las paredes oían. Llegado el teléfono, se "pinchaban" las líneas. Ahora es tanta la actividad que se desarrolla en el ciberespacio, que el espionaje ha invadido también ese dominio.

El ciberespacio, a diferencia de las fronteras materiales de tiempos pasados, es intangible. Las normas, diseños e inversiones que se le apliquen determinarán las formas de interacción entre el espionaje, la salvaguardia de lo privado y la seguridad personal o colectiva. Existe en la actualidad un vigoroso movimiento tendente a otorgar a las actividades de espionaje, de "inteligencia", una posición de privilegio, radicada en la facultad de los poderes públicos de interceptar comunicaciones en el ciberespacio. Es evidente que ello supone una gran ventaja para combatir el delito y el terrorismo.

No son tan obvios, sin embargo, los inconvenientes. Para empezar, la adición de una infraestructura de supervisión tal socavaría el sutil tejido de Internet, una estructura montada "desde la base", idónea para la innovación empresarial. Sus costes podrían obligar a muchos pequeños proveedores de servicios a cerrar sus empresas; por otra parte, el control "desde arriba" quizá privase a EE.UU. del primer puesto en la innovación de las comunicaciones.

Además, al poner un énfasis excesivo en los medios para interceptar las comunicaciones por Internet, tal vez se estén socavando los derechos civiles. Es posible que se ponga en peligro la seguridad del ciberespacio y, en definitiva, la del país. Si se incrusta en los sistemas de comunicaciones un amplio dispositivo de escuchas, ¿cómo se garantizará que no será indebidamente utilizado? Los servicios de policía e inteligencia podrían servirse de él para espiar a sus conciudadanos, sea por corrupción o por mero exceso de celo, vulnerando la Constitución. Y, al igual que con cualquier otro medio de interceptación, cabe el riesgo de que caiga en malas manos. Delincuentes, terroristas o servicios de inteligencia extranjeros podrían infiltrarse en los sistemas de vigilancia y volverlos contra sí mismos. Las medidas preventivas necesarias para protegernos de estas dos amenazas requieren arquitecturas diferentes.

Por su importancia, las cuestiones expuestas son merecedoras de un amplio debate. Mas, desdichadamente, la capacidad de los ciudadanos de participar en tal discusión está muy limitada por el secretismo que envuelve a todas las actividades de espionaje y, en especial, a

HARRY CAMPBELL

CONCEPTOS BASICOS

- La informatización de las centrales telefónicas y la telefonía por Internet le han dificultado a los gobiernos la supervisión de las comunicaciones de delincuentes, espías y terroristas.
- Las agencias federales estadounidenses quieren que las compañías de Internet cumplan los mismos requisitos previstos para la intervención de líneas en las compañías de telecomunicaciones. Esta propuesta puede asfixiar la capacidad de innovación en la Red.
- Además, los nuevos medios de vigilancia podrían ser mal utilizados por funcionarios con exceso de celo o resultar infiltradas por terroristas y espías interesados en supervisar las comunicaciones de los países.

las de interceptación de mensajes (la llamada “inteligencia de señales”).

Historia sucinta de las comunicaciones y de su interceptación

Para comprender la controversia actual sobre las escuchas, es necesario conocer un poco la historia de su técnica. Desde la implantación del teléfono, a finales del siglo XIX, hasta hace unos quince o veinte años, las comunicaciones por voz entre puntos distantes se establecían, casi exclusivamente, mediante sistemas de conmutación de circuitos. Cuando un abonado efectuaba una llamada a otro, una o varias centrales —nodos de la red— se encargaban de conectar sus líneas de modo que se crease un circuito continuo entre los interlocutores. El circuito correspondiente se mantenía durante toda la llamada; a su término, las centrales desconectaban las líneas, dejándolas libres para nuevas solicitudes. Incluso una vez las centrales se transformaron en automáticas, lo único que hacían era conmutar líneas. Otros servicios, como el desvío de llamadas o la recepción de mensajes, estaban a cargo de operadores.

En los EE.UU., la legislación sobre escuchas de telefonía ha ido evolucionando de forma intermitente. Las primeras escuchas consistían en meras derivaciones, tomadas en algún punto de la línea que iba de la central al abonado; el “pinchazo” transmitía la señal hasta unos auriculares y un aparato de grabación. Más adelante, las derivaciones se instalaron en las propias centrales, en las estructuras que soportaban las líneas. Los tribunales, en un principio, sostuvieron que los pinchazos no constituían actos de registro si no invadían el domicilio o propiedades del abonado, pero semejante valoración fue cambiando con el tiempo. En 1967, el Tribunal Supremo estadounidense falló, en el caso *Katz contra EE.UU.*, que la interceptación de comunicaciones sí constituía un registro y, en consecuencia, requería una orden judicial.

Esa decisión motivó que el Congreso estadounidense aprobase en 1968 una ley que estipulaba la autorización judicial para escuchas en investigaciones criminales. Pero la medida aprobada por el Congreso dejaba en el limbo la interceptación de comunicaciones si su finalidad era recabar información del exterior. Las investigaciones del Congreso subsiguientes al caso Watergate (1972) dejaron al descubierto un historial de operaciones, ordenadas desde la Presidencia, que aplicaban tales prácticas de modo abusivo, al espiar a organizaciones políticas pacíficas de su propio país y no sólo a organizaciones extranjeras hostiles.

En consecuencia, el Congreso aprobó una ley sobre las operaciones de vigilancia encaminadas a obtener información acerca de potencias u organizaciones extranjeras (FISA, *Foreign Intelligence Surveillance Act*). Adoptó una medida muy controvertida: la creación de un tribunal federal secreto que habría de emitir los permisos de escucha.

¿Cómo se garantiza que los sistemas de supervisión de comunicaciones no se utilizarán indebidamente?

Casi toda la vigilancia de comunicaciones con la finalidad de obtener información sobre potencias u organizaciones extranjeras quedaba excluida de la ley de escuchas. Se orientaba, sobre todo, a la interceptación de señales de radio y muy poco a intrusiones materiales en los sistemas telefónicos. (Cuando operaban en otros países, los servicios de inteligencia estadounidenses no podían pinchar las líneas de teléfono tan fácilmente como en su país.) Otra importante diferencia entre la vigilancia de comunicaciones en el interior de EE.UU. y en el extranjero es el factor de escala. Tradicionalmente, se ha considerado que la intervención de líneas telefónicas dentro de EE.UU. es una técnica de investigación limitada a delitos muy graves. En lo tocante al exterior, en cambio, la interceptación de comunicaciones alcanza grandes proporciones. En sus operaciones exteriores, la Agencia Nacional de Seguridad (NSA) destina anualmente miles de millones de dólares a la interceptación de comunicaciones, tanto desde bases terrestres como desde barcos, aviones y satélites de espionaje.

Pero las diferencias más importantes son de procedimiento. En el interior de los EE.UU., la Cuarta Enmienda a la Constitución garantiza el derecho de las personas a no ser sometidas a “registros e incautaciones irrazonables”. Para determinar si un registro es “razonable”, los agentes han de efectuar previamente una observación “sin privilegios” (que respete la privacidad del sospechoso),



Una historia de las escuchas

La vigilancia del gobierno ha suscitado muchos problemas legales al irse perfeccionando las comunicaciones por voz.

BETTMAN/CORBIS (*receptor telefónico*); *NEW YORK TIMES*, PAG. 1, 20 DE MAYO DE 1916 (*periódico*); ANGEL FRANCO AP PHOTO (*rótulo Laboratorios Bell*)

de cuyos resultados se deduzca una “causa probable”, un motivo justificado para dirigirse a los tribunales en petición del mandamiento de registro. Lo que no les está permitido, ni para el registro de lugares ni para las escuchas, es empezar por el registro y utilizar después lo que puedan descubrir para demostrar que fue lícitamente efectuado. Ahora bien, es precisamente este segundo procedimiento el utilizado por las agencias de inteligencia, sólo que, de ordinario, sus resultados no se utilizan para la persecución de delincuentes. El agente de inteligencia se basa en su juicio profesional y en la información disponible para tomar la decisión de espiar a un objetivo extranjero; la operación será ulteriormente valorada como éxito o fracaso en función de la información obtenida y de los recursos invertidos.

Las normas de la ley FISA determinan tres diferencias fundamentales: entre “U.S. persons” (ciudadanos estadounidenses, residentes legales y corporaciones con sede en EE.UU.) y extranjeros; entre comunicaciones en el interior y en el exterior de EE.UU., y entre comunicaciones alámbricas y comunicaciones inalámbricas. En breve: las comunicaciones mediante líneas alámbricas enteramente contenidas en el interior de EE.UU. se hallan totalmente protegidas por la ley; su intervención exige un mandamiento judicial. Pero las comunicaciones por radio en las que participen personas en el exterior del país sólo se hallarían protegidas si la señal fuese interceptada en el interior de EE.UU. y el presunto objetivo fuese un individuo particular, una “U.S. person” identificada como tal, que se encontrase en el país en ese momento.

Hasta hace poco, dondequiera que fuesen de aplicación las normas de FISA, éstas imponían exigencias similares a las de la jurisdicción criminal ordinaria. Para solicitar un mandamiento, la agencia de inteligencia había de especificar una ubicación concreta y explicar las razones por las que la persona objetivo había de ser sometida a vigilancia. No es lícito actuar como cuando se espía a extranjeros, ni interceptar comunicaciones y utilizar después las correspondientes grabaciones para justificar la intervención efectuada.

Casi fortuitamente, las normas establecidas por FISA contenían un importante vacío legal, que el Congreso había pretendido que sólo tuviera carácter transitorio: las comunicaciones con participación de personas no estadounidenses podrían ser interceptadas sin mandamiento judicial desde el interior de EE.UU. En el momento en que FISA fue aprobada, y durante muchos años después, esta norma de exención, presuntamente transitoria, constituyó una bendición para los servicios de inteligencia.

En los años sesenta y setenta, se produjo una revolución en las comunicaciones internacionales, fruto de los satélites repetidores, que se encargaban de casi todas las comunicaciones entrantes o salientes de EE.UU. Las radiocomunicaciones entre interlocutores que estuvieran ubicados, total o parcialmente, en el exterior de los EE.UU. eran legal y físicamente vulnerables a la interceptación por antenas de la NSA instaladas en lugares como Yakima, en el límite noroccidental del país, o en Vint Hills Farms, en Virginia, en la costa atlántica.

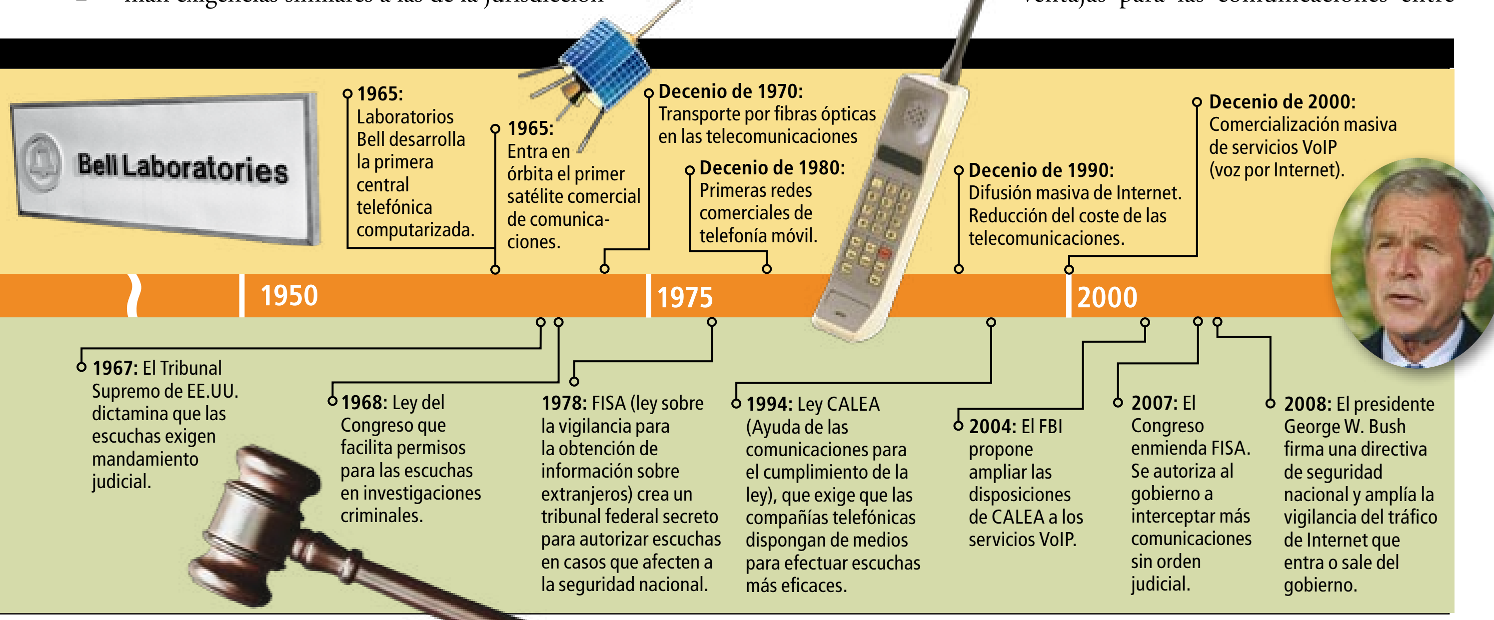
Pero en los años setenta apareció un nuevo medio de transmisión de grandes cantidades de información. Las fibras ópticas, filamentos de vidrio muy largos y delgados, adecuados para la transmisión de señales mediante luz láser, presentaban grandes ventajas para las comunicaciones entre

MINIMIZACION

Una de las principales diferencias de procedimiento entre las escuchas contra la delincuencia y la vigilancia de elementos extranjeros por los servicios de inteligencia estriba en una práctica llamada minimización: evitar que se recojan informaciones no pretendidas. Varias personas pueden utilizar una línea telefónica pinchada, por ejemplo, algunas de las cuales no son objeto de la investigación.

Las leyes estadounidenses exigen que la policía escuche las conversaciones a la vez que se procede a grabarlas, y que cese la vigilancia cuando los sujetos no estén tratando de actividades delictivas.

En la recolección de información del exterior, las reglas de minimización no son, por lo general, tan rígidas, pero debido a que son tantas las señales que pueden ser interceptadas y analizadas, el tráfico que ha de ser desechado por irrelevante es muchísimo mayor.

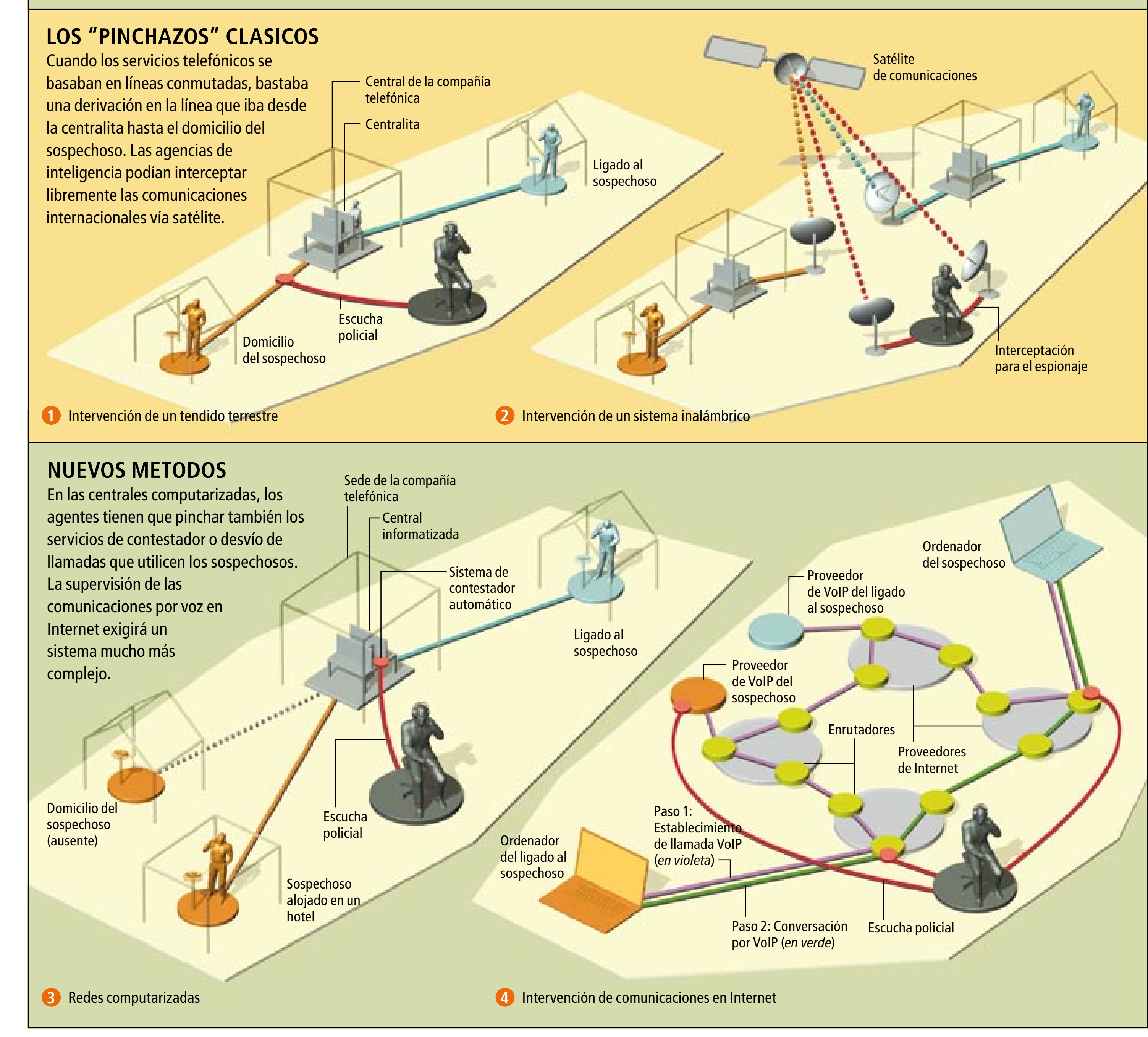


DAVID MUIR (*mazo*); JEN CHRISTIANSEN (*satélite*); LAWRENCE MANNING CORBIS (TELÉFONO); ROGER L. WOLLENGERG *Pool/CNP/Corbis* (*Bush*)

dos puntos fijos. Su capacidad de transporte es colosal; no se sufren las molestas demoras de un cuarto de segundo que ralentizan las conversaciones vía satélite; son intrínsecamente más seguras que los sistemas de radio; y por una conjunción de razones técnicas, su coste es muy reducido.

A partir de los años noventa, la gran mayoría de las comunicaciones entre ubicaciones fijas se efectúa mediante fibras. Y puesto que estas comunicaciones son "alámbricas", vale decir, mediante tendidos permanentes, las leyes estadounidenses les otorgan mayor protección. Los servicios de inteligencia ya no podían escuchar estas comunicaciones con tanta libertad como solía con las señales radioeléctricas. Las normas de FISA empezaron a resultarles un auténtico fastidio.

Materia de especial interés para las agencias de espionaje era el llamado "tráfico de tránsito". Alrededor del 20 por ciento de las comunicaciones que transportan las redes es-



tadounidenses se originan y concluyen fuera de ese país, y se desplazan entre Europa, Asia o las Américas Central y del Sur. El tráfico en tránsito no constituye un fenómeno nuevo: ya acontecía en la era de los satélites. Pero con las regulaciones de FISA, la interceptación de comunicaciones por fibra en el interior de EE.UU. exigía un mandamiento judicial. Este requisito suponía un oneroso obstáculo para los procedimientos habituales de los agentes de inteligencia, no habituados a buscar justificaciones ni "causas probables" antes de iniciar la vigilancia.

Aproximadamente por entonces, las centrales telefónicas tradicionales de las redes telefónicas norteamericanas, de conmutación electromecánica, empezaron a ser sustituidas por centrales computarizadas. Su informatización abrió el camino a servicios como el desvío de llamadas o el contestador automático, que de forma no intencionada, pero sí muy eficaz, permitían eludir las escuchas tradicionales. Supongamos, por ejemplo, que se deposite un mensaje en un contestador facilitado por la compañía telefónica. Si el abonado consulta sus mensajes desde un teléfono que no sea el propio, aunque su línea esté pinchada, la comunicación nunca viajará por ella y, en consecuencia, no será interceptada. El Congreso respondió en 1994 con la ley CALEA (*Communications Assistance for Law Enforcement)* de ayuda de las comunicaciones al cumplimiento de la norma, que exige que las compañías de comunicaciones le faciliten al gobierno la supervisión de todas las comunicaciones de abonados sospechosos, cualesquiera que sean los servicios automáticos que utilicen. Además de ordenar una mejora en la calidad de las informaciones que se obtienen de los pinchazos, la CALEA obligaba a las compañías de telecomunicaciones a poseer la capacidad técnica de efectuar muchas más intervenciones simultáneas de lo que antes era posible.

Pinchazos en la Red

CALEA se aprobó justamente cuando empezaba a ser general el uso de Internet, donde las comunicaciones se efectúan de modo totalmente diferente de la conmutación de circuitos. En Internet, la información se envía por paquetes pequeños, dotados cada uno de una dirección de destino y de una dirección de remitente, lo mismo que las cartas enviadas por el servicio de correos. En el caso de la conmutación de circuitos, el coste del establecimiento de comunicación es el mismo, sea de breve o larga duración la llamada, por lo que efectuar una llamada para enviar unas cuantas palabras no resulta económico. Pero en una red de conmutación por paquetes, los mensajes cortos son baratos, y lo son tanto más cuanto mayor sea su brevedad. La navegación por la Red resulta posible porque las conexiones de Internet pueden utilizarse durante poco tiempo y descartarse después. Cada vez que hacemos clic sobre un enlace, se establece en la Red una conexión nueva.

En la era de la conmutación de circuitos, los pinchazos resultaban eficaces porque los aparatos telefónicos, los números de los abonados y los propios usuarios se hallaban estrechamente vinculados. Cambiar el emplazamiento de un teléfono no resultaba fácil y obtener un número nuevo, lento y dificultoso. Los mensajes de las organizaciones circulaban por unos mismos canales durante largos períodos, por lo que resultaba sencillo interceptarlos repetidamente. La conmutación computarizada e Internet han hecho mucho más compleja la supervisión de las comunicaciones. En nuestros días no cuesta obtener nuevos números de teléfono, así como nuevas direcciones de correo electrónico, pseudónimos de mensajería instantánea y otros elementos de identidad. Y el advenimiento del protocolo VoIP (voz sobre Internet), el estándar que permite la transmisión de voz sobre redes de conmutación por paquetes, ha descentralizado todavía más el control sobre las infraestructuras de comunicaciones. En un sistema VoIP, así el popular Skype, el establecimiento de llamadas telefónicas y el tráfico asociado a la conversación se hallan totalmente separados.

Si CALEA, en su interpretación literal, se aplicase a servicios VoIP descentralizados, al proveedor se le exigiría que interceptase las llamadas telefónicas de los individuos que le fueran indicados y las retransmitiese a los servicios gubernativos, una exigencia quizás imposible de cumplir. Tomemos, por ejemplo, una llamada por VoIP efectuada a través de los ordenadores personales de dos individuos que se encuentran de viaje. Alicia inicia la llamada desde una sala del aeropuerto O'Hare de Chicago y Bob la recibe en el bar de un hotel en San Francisco. El papel del proveedor de VoIP en este proceso es limitado: averiguar las direcciones IP (protocolo de Internet) desde las que se van a conectar los ordenadores de Alicia y Bob y comunicar al ordenador de cada uno la dirección del otro. Una vez ejecutados estos procedimientos, el proveedor de VoIP no desempeña papel alguno. La auténtica conversación de voz es transportada por los respectivos proveedores de servicios de Internet (ISP) por cuyo intermedio acceden a la Red Alicia y Bob, así como por los otros transportistas de datos a los que dichos ISP se encuentren conectados.

Los autores

Whitfield Diffie comenzó su carrera en seguridad informática como inventor de la idea de criptografía de clave pública. En el decenio pasado dirigió su atención hacia la política pública y desempeñó un papel crucial en la oposición a los deseos del gobierno de contar con un registro de claves y de imponer normas restrictivas a la exportación de productos que incorporasen sistemas de cifrado. En la actualidad es jefe de seguridad en Sun. **Susan Landau** es ingeniera del Sun Microsystems Laboratory, donde se ocupa de la vigilancia y de la gestión de elementos de identificación. Con anterioridad, Landau había sido miembro de la Universidad de Massachusetts en Amherst y de la Universidad Wesleyana, donde trabajó en algoritmos algebraicos.

GEORGE RETSECK

En este ambiente, para supervisar tan sólo a un objetivo, los organismos gubernativos tendrían que presentarles mandamientos de vigilancia a muchos transportistas de telecomunicaciones. Imaginemos un régimen de interceptación de estilo CALEA que pudiese captar llamadas de VoIP. Tiene que empezar dirigiendo una orden al proveedor de VoIP, sea el de Alicia o el de Bob. Cuando los funcionarios gubernativos sean informados por este proveedor de que la "diana" participa en una llamada, han de considerar las direcciones IP de Alicia y de Bob y enviar mandamientos de interceptación a uno o varios ISP en los que resulte posible intervenir la conversación. Los ISP correspondientes tienen que estar preparados para aceptar el mandamiento, verificar su autenticidad y ejecutar la interceptación, todo ello al instante, "en tiempo real". Otra de las dificultades de este supuesto es que sólo se les podría exigir la obediencia al mandamiento a las ISP ubicadas en EE.UU. (y posiblemente, a las de algunos países dispuestos a colaborar). Mayor entidad todavía tiene el colosal problema de seguridad que presentaría un planteamiento semejante, pues quien fuera capaz de infiltrarse hasta los medios de intervención de un ISP podría espiar a voluntad a sus abonados.

CALEA reconoció la diferencia entre la telefonía tradicional e Internet, eximiendo a Internet, a la que se refiere como "servicios de información", de las disposiciones de la nueva ley. A pesar de esta exención, el Departamento de Justicia de los EE.UU., el FBI y la DEA (agencia contra el tráfico de drogas) respondieron al problema de la supervisión de comunicaciones por Internet con la propuesta de que los proveedores de banda ancha de Internet tuvieran también que cumplir las disposiciones de CALEA. La Comisión Federal de Comunicaciones (FCC) y los tribunales han respaldado hasta ahora a los organismos policiales, y han extendido CALEA a la "VoIP interconectada" (lo más parecido a la telefonía tradicional) basándose en un artículo de CALEA alusivo a servicios que reemplacen de forma sustancial al sistema telefónico. De ser aceptada la propuesta, se habría dado el primer paso por un camino que conlleva graves peligros, no existentes en los métodos tradicionales.

En particular, las acciones del gobierno constituyen una amenaza para el crecimiento regular de Internet, que se ha convertido en vivero de innovaciones gracias a su control distribuido y a su flexible conectividad. A diferencia de las redes tradicionales de transporte de telefonía, Internet no está planificada ni gestionada de forma centralizada. En el sistema telefónico, la adición de servicios nuevos, como el desvío de llamadas, suele exigir años de planificación y desarrollo. Pero en Internet, un emprendedor puede poner en marcha una pequeña empresa nacida en un garaje o en el cuarto de su residencia de estudiantes utilizando sólo un ordenador personal y una conexión de banda ancha. Si la ley consigue imponer instalaciones de interceptación a cada compañía de Internet, la industria en su conjunto acabará yaciendo en el lecho de Procrusto de las telecomunicaciones ordinarias. Para incorporar amplias capacidades de vigilancia, los nuevos servicios de Internet tendrían que desarrollarse en ciclos largos, dependientes de la administración federal. Estados Unidos podría rezagarse con respecto a países que tomasen una senda diferente. Tal resultado sí que supondría a largo plazo una grave amenaza para la seguridad nacional.

Existe otra amenaza más inmediata. Desde que se derrumbó la Unión Soviética, ningún oponente ha dispuesto de capacidad para espiar las comunicaciones de EE.UU. con nada que se aproxime a una cobertura completa. Los soviéticos contaban con flotas de buques arrastreros que patrullaban por ambas costas de EE.UU., de servicios diplomáticos en las grandes ciudades norteamericanas, de satélites en los cielos y de bases terrestres, como las instalaciones de Lourdes, cerca de La Habana. Sus capacidades en cuanto a inteligencia de señales no eran inferiores a las de nadie. En cambio, Al Qaeda, e incluso grandes países, como China, carecen en este momento de semejante capacidad. Pero están tratando de conseguirla.

Geografía de las escuchas

La ley FISA (sobre la vigilancia para la obtención de información sobre extranjeros), enmendada en 2008, detalla qué comunicaciones quedan bajo protección legal, y cuáles se pueden intervenir sin orden judicial.

- Personas de EE.UU. (ciudadanos, con residencia legal, corporaciones de EE.UU.)
- Persona no-EE.-UU.
- Tendido terrestre (*línea continua*)
- Enlace inalámbrico (*línea de puntos*)
- Comunicación protegida (intervenida sólo por orden judicial)
- Comunicación no protegida (su escucha es lícita)

Todas las comunicaciones de las que se sepa que se realizan por completo dentro de los EE.UU. están protegidas.

Sin embargo, ciertas comunicaciones entre ciudadanos estadounidenses pueden no estar protegidas si tienen origen fuera de los EE.UU.

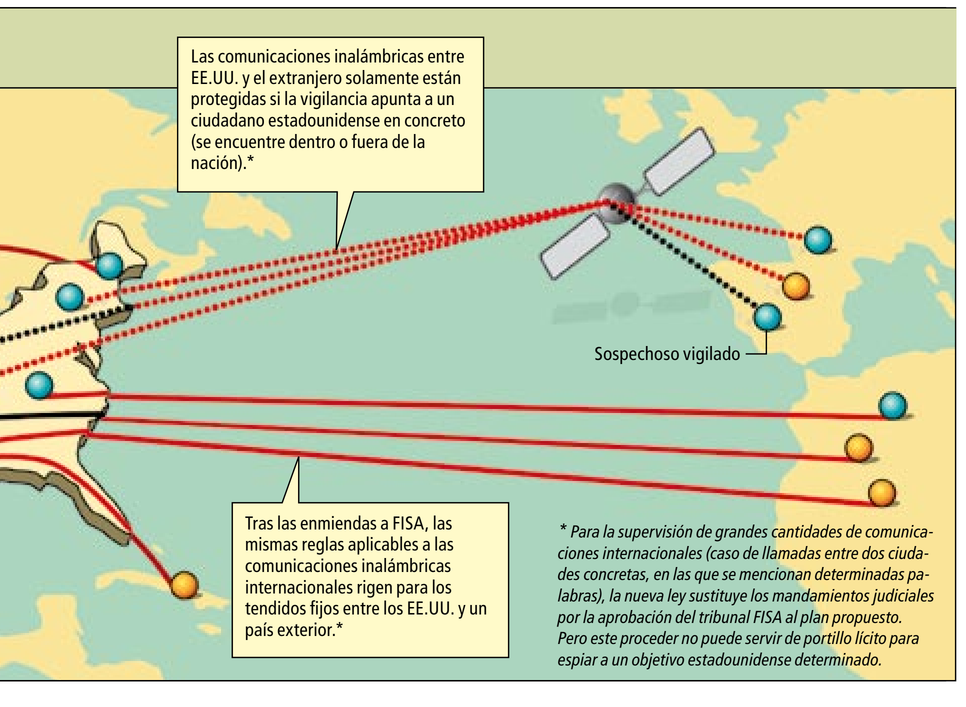
Sospechosos vigilados

El tráfico inalámbrico en tránsito no está protegido en el interior de EE.UU.

Enmiendas recientes a FISA establecen que el tráfico en tránsito por líneas terrestres de EE.UU. no está protegido.

JEN CHRISTIANSEN

La comunicación, en nuestra especie, es fundamental. Y en la comunicación es fundamental la privacidad, tanto para la seguridad nacional como para la democracia.



La integración en Internet de sistemas de supervisión podría facilitársela. Los dispositivos de interceptación estarían controlados mediante ordenadores, los cuales, a su vez, estarían controlados a distancia. Tales sistemas podrían ser tan susceptibles de captura como los sitios de la Red o los ordenadores personales. Las políticas de interceptación que propone el gobierno de Estados Unidos han de ser valoradas a esa luz.

Ciberguerras

La administración del presidente George W. Bush relajó hace poco algunas de las restricciones a la supervisión de las comunicaciones estipuladas por la ley FISA, en vigencia desde hacía 30 años. En 2007, el Congreso, bajo intensa presión desde la Casa Blanca, aprobó la Ley de Protección de América (PAA), que enmendaba la FISA al ampliar a todas las comunicaciones las excepciones que FISA reservaba para la radio. La nueva ley establecía que toda comunicación que razonablemente pudiera contar con interlocutores en el exterior de los EE.UU. era susceptible de interceptación sin mandamiento judicial previo. En vista del grado en que los servicios comerciales estadounidenses se están subrogando a empresas de ultramar, esta ley abría las puertas a la supervisión discrecional de gran parte de las telecomunicaciones comerciales o personales de los estadounidenses. Tan grandes eran los recelos del Congreso ante esta línea de actuación, que estaba previsto que la PAA fuese una ley transitoria y derogada en 2008.

En julio de 2008, tras meses de controversia, el Congreso aceptó una propuesta de ley que ampliaba la autoridad del Ejecutivo para ordenar escuchas y reducía el papel del tribunal FISA en casos internacionales a la revisión de los procedimientos generales de las escuchas propuestas, en lugar del examen de los detalles concretos de cada caso. Empero, el debate político no estuvo centrado, como sería de esperar ante una propuesta tan radical, en cuál sería la autoridad que pudiera ordenar las escuchas. Casi toda la atención recayó sobre la concesión de inmunidad, con efectos retroactivos a las escuchas ilegales del pasado.

A comienzos de 2008, la Administración ofreció una nueva justificación de la ampliación de la vigilancia sobre las comunicaciones: garantizar la seguridad de Internet. Ciertamente, en la actualidad la seguridad de Internet se halla en un estado lamentable. La mayoría de los ordenadores no disponen de suficiente protección frente al *malware*: programas diseñados para infiltrarse en los sistemas informáticos a fin de dañarlos o controlarlos. Y una proporción importante de los ordenadores conectados a Internet se encuentra bajo el control de terceros que no son sus propietarios. Estas máquinas han sido capturadas y organizadas subrepticiamente en *botnets* —redes de "robots" de Internet—, cuya capacidad computacional es revendida en una especie de mercado de esclavos electrónicos.

Ante el fracaso de los métodos defensivos tradicionales, el Presidente Bush firmó una directiva de seguridad nacional autorizando una "iniciativa cibernética", la Cyber Initiative. La mayor parte de dicha directiva es secreta, pero su primera medida —una vigilancia generalizada de la importante cantidad de tráfico de Internet que entra y sale de los organismos gubernativos de EE.UU.— abarca demasiado para que se pueda ocultar. Al objeto de facilitar tal vigilancia, la Administración proyecta reducir el número de conexiones entre organismos gubernativos e Internet desde los millares actuales hasta menos de un centenar, lo que exige la modificación o eliminación de miles de direcciones IP. La iniciativa cibernética capta a la perfección el dilema de la inteligencia de señales. Un sistema que supervise las comunicaciones federales en busca de intrusiones por extranjeros va a captar necesariamente todas las comunicaciones legítimas que los ciudadanos mantienen con su gobierno.

La Administración se propone disponer del poder de interceptar las comunicaciones entre estadounidenses valiéndose de las mismas tácticas largo tiempo utilizadas para recopilar información sobre extranjeros, es decir, sin tener que recurrir a los tribunales en solicitud de mandamientos ni de explicaciones

La interceptación de las comunicaciones en España

El derecho de la privacidad de las comunicaciones forma parte de la Declaración de Derechos Humanos y se recoge de manera expresa en las Constituciones de la mayoría de los países. Sin embargo, en las legislaciones internas, incluso en países democráticos, se recogen algunas excepciones con el argumento de que son necesarias para la seguridad nacional. En estos casos de excepción hay autores que consideran que la razón de Estado supone una transgresión de la moral y la justicia.

En España sólo hay una legislación clara, aunque parcial, a partir de mayo de 2002, por la Ley que regula el funcionamiento del Centro Nacional de Inteligencia (CNI), que establece que este organismo necesita la autorización previa de un juez del Tribunal Supremo para intervenir legalmente las comunicaciones. Sin embargo, no están regulados en este sentido los servicios de información de la Policía y de la Guardia Civil, que no tienen una legislación específica al respecto. Además, la autorización judicial previa, necesaria para el CNI, tampoco afecta a los servicios de los tres Ejércitos.

En las relaciones internacionales la regulación es aún más difícil y difusa, ya que sólo existen algunas declaraciones con poca fuerza jurídica, como la del Parlamento Europeo que considera que toda escucha de las comunicaciones es una violación grave de la intimidad de la persona.

Juan José Prieto
Asesor científico para seguridad y defensa
del Ministerio de Ciencia e Innovación

previas sobre lo que se propone interceptar. La inquietud de quienes abogan en favor de la ampliación de la vigilancia tiene un fundamento: no sólo se enfrentan a oponentes no vinculados a países concretos, a individuos que pueden desplazarse libremente por los EE.UU. y entrar o salir de ellos; padecen además un problema crítico de ciberseguridad. Internet se está convirtiendo rápidamente en el medio principal para la gestión gubernativa en lo que concierne a las empresas privadas; para muchos individuos constituye también la vía de comunicación preferida. Sus problemas de seguridad se asemejan a los de tiempos pasados: caminos infestados de salteadores o vías marítimas controladas por piratas. En tales circunstancias, no es sorprendente que el gobierno pretenda patrullar Internet, exactamente igual que las distintas policías y los servicios armados han patrullado los caminos o los mares en el pasado.

Pero al someter Internet a vigilancia policial, en lugar de buscar la seguridad de los ordenadores que moran en ella, puede ocurrir que el remedio sea peor que la enfermedad. ¿Van a ser los instrumentos gubernamentales de supervisión más seguros que las redes que están tratando de proteger? De no ser así, los servicios de vigilancia corren el riesgo de que se los pervierta e incluso que se los vuelva contra sí mismos. Los problemas de seguridad que hoy son la maldición de Internet pueden afectar por igual a los ordenadores encargados de la vigilancia y a los ordenadores que están siendo vigilados. Si el gobierno de Estados Unidos amplía sus facultades para husmear en Internet sin resolver previamente los problemas de seguridad que sufren los ordenadores, buscará el desastre.

Los peligros intrínsecos se agravan por el secretismo que envuelve a las iniciativas del gobierno. Entre las víctimas de las recientes metodologías de interceptación de comunicaciones se cuenta la "regla de las dos organizaciones". La seguridad de muchos sistemas cruciales, como en el caso de los que controlan armas nucleares, se funda en la duplicación: así, por ejemplo, la exigencia de que dos personas tengan que efectuar simultáneamente una acción de importancia crítica.

Hasta no hace mucho, una ley federal ordenaba que los pinchazos obedecieran a principios similares, pues si permitía que el gobierno emitiera las órdenes de escucha, exigía en cambio que fuesen las compañías telefónicas las que instalasen los pinchazos. Las compañías telefónicas se mostrarían reacias a obedecer tales órdenes, si sospechasen que no eran legales, pues de acceder, podrían incurrir en delito. Al suprimir el papel de las compañías telefónicas se elimina una importante salvaguardia. Si seguimos por este camino, quizá creemos un régimen totalmente opaco al Congreso, a los tribunales y a la prensa, y quién sabe si totalmente fuera de control.

La incursión en el ciberespacio que nuestro mundo efectuó en el siglo XX resultará mínima en comparación con la que va a realizar en el siglo XXI o los siguientes. Nos encontramos en el proceso de construir el mundo en el que van a habitar los seres humanos del futuro, un proceso similar al de hace 5000 años, cuando nacieron las primeras ciudades. La comunicación, en nuestra especie, es fundamental. Y en la comunicación es fundamental la privacidad, tanto para la seguridad nacional como para la democracia. El gran reto que hemos de afrontar es la conservación de dicha privacidad, estando inmersos en nuevas técnicas de comunicación y rodeados de graves amenazas a la seguridad colectiva. Pero es de crítica importancia que nuestras decisiones respeten la intimidad de las personas, la seguridad de las comunicaciones y la capacidad de innovación. Si no, se esfumará toda esperanza de tener una sociedad libre.

Bibliografía complementaria

INFORMATION PRIVACY LAW: CASES AND MATERIALS. Segunda edición. Daniel J. Solove, Marc Rotenberg y Paul Schwartz. Aspen, 2005.

SECURITY IMPLICATIONS OF APPLYING THE COMMUNICATIONS ASSISTANCE TO LAW ENFORCEMENT TO VOICE OVER IP. Steven M. Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Diffie, Susan Landau, Jon Peterson y John Treichler. *Information Technology Association of America*, 2006.

PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION. Edición actualizada y ampliada. Whitfield Diffie y Susan Landau. MIT Press, 2007.

Puede consultarse más información relativa a vigilancias en los sitios que tiene en la Red el Centro para la Democracia y Tecnología (Center for Democracy and Technology): www.cdt.org; la Fundación Frontera Electrónica (Electronic Frontier Foundation): www.eff.org; y el Centro de Privacidad de la Información (Electronic Privacy Information Center): www.epic.org

Leones marinos de ciudad

Montse García, Josep-Maria Gili

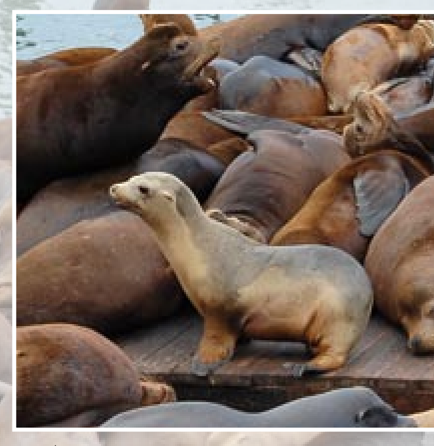
Por culpa de la sobreocupación del litoral, muchas especies marinas que solían utilizar la zona costera para sus asentamientos habituales se han visto obligadas a buscar soluciones alternativas. En algunos casos, la solución ha conllevado el uso de hábitats artificiales, creados por el hombre, como puertos marítimos y otras obras de ingeniería.

Constituye un buen ejemplo de este fenómeno el león marino de California (*Zalophus californianus*). La colonia más visible de esta especie es la que se asienta, de forma permanente desde 1990, en el espigón 39 del puerto de San Francisco. Si bien la especie presenta una amplia distribución geográfica en el océano Pacífico, cada población local vive aislada de las otras. En la actualidad, estas grandes colonias se encuentran en peligro puesto que, al alimentarse sobre todo de peces, representan una amenaza para las capturas de los pescadores.

El león marino de California se ha convertido en una especie indicadora de los cambios y del estado del ecosistema marino. Hallar un equilibrio entre el mantenimiento de estas poblaciones y la explotación de los recursos naturales constituye un reto de primer orden para nuestra sociedad.



1. Colonia de leones marinos de California en el espigón 39 del puerto de San Francisco. A lo largo del año se concentran aquí miles de ejemplares de los 200.000 que integran el total de la población.



▲ 2. Los cachorros de león marino nacen a comienzos del verano, tras once meses de gestación. Cada hembra engendra un cachorro que amamanta durante alrededor de un año. Es el único mamífero cuya leche no contiene lactosa.

◀ 3. Los machos pueden pesar más de 200 kilogramos y superan los 2 metros de longitud. Muestran un pelaje negruzco. Alcanzan la madurez sexual a los 4 años y medio; pueden vivir hasta 25 años.

4. Las hembras, con más de 100 kilogramos, alcanzan los 2 metros de longitud. Presentan un pelaje marrón. Viven en pequeños harenes dominados por un macho. ▼

MONTSE GARCIA Y JOSEP-MARIA GILI

Jeremy Nicholson: el hombre de las bacterias intestinales

Jeremy Nicholson ha descubierto que el cuerpo y su flora intestinal producen sustancias químicas que atesoran información sobre la salud. Puede que llegue el día en que para tratar muchas enfermedades tengamos que ocuparnos de esas bacterias

Melinda Wenner

Jeremy Nicholson sólo quería ser riguroso. Corría 1981. El joven bioquímico trabajaba con espectroscopía por resonancia magnética nuclear, técnica que permite identificar las sustancias químicas a partir de las propiedades magnéticas de los núcleos atómicos. En particular, Nicholson deseaba estudiar el modo en que los glóbulos rojos absorbían el cadmio, un metal cancerígeno. Sabedor de que obtendría los mejores resultados si conseguía reproducir el hábitat natural de las células, les añadió unas pocas gotas de sangre y llevó a cabo la prueba.

"De repente, aparecieron señales de lo más variopinto y que nunca habíamos visto, toda una sorprendente serie de espectros", recuerda. Una muestra de sangre o de orina contiene miles de metabolitos, huellas de todas las reacciones químicas que tienen lugar en el cuerpo en un momento dado. Si pudiera encontrar la manera de identificar todas esas improntas químicas y conocer su relevancia, razonó, no sólo conocería mejor las enfermedades (a partir de las reacciones químicas que se descontrolan), sino también de identificar las señales precursoras y qué intervenciones serían factibles. Y quedó prendado de esa clase de ciencia.

Hoy día Nicholson, a sus 51 años, es uno de los mayores expertos mundiales en metaboloma, conjunto de sustancias químicas resultantes del metabolismo humano. Si el genoma suministra una información detallada sobre la constitución genética de una persona, el metaboloma se sitúa unos pasos más allá: pone de manifiesto la interacción entre genes y entorno, proporcionando una instantánea completa de la salud física de un sujeto. "El genoma viene a ser como una guía telefónica en la que faltasen los nombres y las direcciones. A un nivel elemental, lo que contiene es un montón de números", explica Nicholson, que dirige el departamento de medicina molecular del Colegio Imperial de Londres. El metaboloma "sirve para proveer de significado a la información del genoma y ponerla en perspectiva".

Pero primero debe descifrarse, tarea nada baladí. Requiere análisis de sangre, orina, aliento y heces de una población muy numerosa. Por poner un caso, para encontrar huellas químicas prometedoras (marcadores biológicos) de la hipertensión arterial, Nicholson y sus colegas analizaron la orina de 4630 individuos procedentes del Reino Unido, Estados Unidos y Asia, y cotejaron los metabolitos de la orina con datos de la presión arterial para determinar si existía alguna diferencia metabólica consistente entre los individuos que tenían tensión alta y los que no.

Da la impresión de que su ciencia empieza por el tejado: en vez de formular hipótesis y después diseñar experimentos para comprobarlas, él primero lleva a cabo los experimentos y luego intenta descifrar los resultados. Debe examinar todo el abanico de sustancias químicas producidas por los genes que poseen los individuos, por la comida que ingieren, por las medicinas que toman, por las enfermedades que sufren y por las bacterias intestinales que albergan.

Estas bacterias en particular han llegado a ser el prin-



SION TOUHIG

JEREMY NICHOLSON

PISTAS BACTERIANAS: Nicholson se propone elaborar nuevos útiles de diagnóstico y dianas inéditas para las medicinas gracias al análisis de los productos de las bacterias del intestino.

VASTA POBLACION: El tracto intestinal contiene unos 10 billones de bacterias pertenecientes a unas 1000 especies diferentes.

PADRE DE DISCIPLINAS: Los trabajos de Nicholson han generado dos nuevos campos: la metabolómica, que estudia los metabolitos resultantes de los procesos celulares, y la metabonómica, que caracteriza los cambios metabólicos que experimenta un sistema biológico en respuesta a las solicitaciones externas.

CRECIMIENTO INTERIOR: Sobre su descubrimiento de la impronta metabólica que dejan las células: "Me tenían harto, pensaba que eran interferencias con la bioquímica de los mamíferos. Ahora soy casi un fanático suyo".

cipal interés de Nicholson. Influyen sobre la manera en que nuestros cuerpos disocian los alimentos y las medicinas y puede que den razón de por qué la misma comida le afecta a cada uno de forma diferente. Algunas personas, por ejemplo, no asimilan uno de los componentes de la soja porque en su tracto intestinal carecen de ciertos microorganismos necesarios para procesarlo. Aunque descifrar qué metabolitos proceden directamente de los microorganismos de nuestro intestino puede resultar difícil, en ciertos casos es elemental: son los compuestos químicos que ni son producidos por nuestras células ni provienen de los alimentos ingeridos.

A Nicholson le atraen estos compuestos por lo poco que de ellos se sabe, así como por la gran relevancia que parecen tener: algunas investigaciones sugieren que los microorganismos del intestino desempeñan un cometido crucial en la salud y la enfermedad del ser humano. Nos ayudan a absorber nutrientes y a rechazar virus y bacterias perjudiciales; perturbar las colonias intestinales, como hacen los tratamientos antibióticos, con frecuencia provoca trastornos digestivos. De hecho, dice Nicholson, "casi todas las clases de enfermedades están relacionadas de alguna manera con un microorganismo intestinal".

Quizás el más conocido de los organismos intestinales nocivos sea la bacteria *Helicobacter pylori*, que puede desencadenar úlcera péptica. En los últimos años, los científicos han relacionado la obesidad con la abundancia relativa de dos filos bacterianos dominantes en el intestino, y descubrieron que la presencia de trastornos en las bacterias intestinales está asociada con la grasa hepática no alcohólica, patologías inflamatorias intestinales y algunos tipos de cáncer. Nicholson especula que esos organismos podrían incluso intervenir en ciertas enfermedades neurológicas, como el trastorno por déficit de atención con hiperactividad, el síndrome de Tourette y el autismo. "Disponemos de algunos datos que nos indican que enredar con los microorganismos intestinales repercute en la química del cerebro", señala. Actualmente colabora con microbiólogos para emparejar metabolitos a bacterias concretas; se piensa que cada uno albergamos 1000 especies de bacterias y más de 10 billones de individuos.

Este proceso de identificación sólo es posible desde hace poco. Aunque se extraen bacterias intestinales de las muestras de heces desde hace muchos años, resultaba casi imposible cultivarlas después, pues sólo sobreviven en ambientes muy ácidos y anóxicos. Gracias a las nuevas técnicas de secuenciación de ADN, podemos identificar las bacterias del tracto intestinal de manera bastante sencilla. El interés en esta tarea no para de aumentar: los Instituto Nacionales de la Salud de los Estados Unidos lanzaron el pasado mes de diciembre el proyecto Microbioma Humano, con el objetivo de caracterizar la flora intestinal humana.



COMPAÑEROS DE POR VIDA: *Helicobacter pylori* (*en rojo*) y otras bacterias intestinales condicionan la salud.

PHOTO RESEARCHERS, INC.

Una vez que los investigadores consigan correlacionar los metabolitos con la salud, cabría pensar en confeccionar tiras de orina, similares a las que se utilizan en las pruebas de embarazo, para comprobar de manera regular el estado de nuestra flora intestinal. Algunas empresas han comenzado a vender productos alimenticios para ayudar a mantener en forma estas poblaciones, ya sea con bacterias beneficiosas vivas (alimentos probióticos), ya con compuestos que promueven su crecimiento (prebióticos), ya con combinaciones de ambos (simbióticos).

Lamentablemente, todos estos preparados caen dentro de la categoría de "alimentos funcionales", que no suelen someterse a pruebas clínicas. Una excepción es VSL #3, una combinación de ocho especies de bacterias que la compañía VSL Pharmaceuticals (con sede en Gaithersburg, Maryland) vendía en paquetes. En pruebas doble ciego con grupos de control a los que se administraba placebo, estas colonias pusieron remedio eficaz a la colitis ulcerosa y el síndrome de irritación intestinal.

Nicholson mantiene que son muchas las posibilidades en lo que se refiere a los medicamentos orientados a los microorganismos, cuya apremiante necesidad resulta palmaria. Según un estudio publicado por los laboratorios farmacéuticos Pfizer, el genoma humano ofrece sólo unas 3000 dianas potenciales para los medicamentos, porque únicamente un subconjunto de genes produce proteínas a las que se puedan ligar las moléculas de los medicamentos. Pero "hay un número de genes 100 veces mayor en la flora microbiana", aclara Nicholson, que trabaja asiduamente con los laboratorios farmacéuticos para elucidar el modo en que las personas metabolizan las medicinas. Es "uno de los pocos académicos que conozco que se interesa en la industria farmacéutica más por sus problemas que por su dinero", señala Ian Wilson, un científico que trabaja en Inglaterra para AstraZeneca. Wilson añade que Nicholson nunca se queda sin soluciones, y lo califica de "una masa de ideas en ebullición".

Como los genes proporcionan sólo una información limitada sobre el riesgo que corre el individuo de contraer una enfermedad, Nicholson sueña con el momento en el que se pueda proporcionar un tratamiento personalizado para cada metaboloma. Sencillos análisis de sangre o de orina podrían detectar el riesgo de cáncer o de trastornos cardiovasculares con la suficiente antelación como para emprender una terapia preventiva; las medicinas se adaptarían al perfil metabólico de cada persona, y en muchos casos actuarían, no sobre nuestros órganos, sino sobre nuestras bacterias. "Se abre una visión del futuro que no habríamos sospechado hace pocos años", dice Nicholson. "Muchos microbiólogos pueden aducir que no son más que sueños, pero en la ciencia sólo se realizan grandes progresos cuando nos atrevemos a imaginar lo inimaginable."

Reaparece el fantasma de Malthus

Todavía está por ver si sus famosas predicciones pesimistas fueron erróneas o sólo prematuras

Jeffrey D. Sachs

En 1798, el economista Thomas Robert Malthus afirmaba, en sus famosas predicciones, que las mejoras a corto plazo del nivel de vida declinarían inevitablemente cuando el crecimiento de la población superara el de la producción de alimentos; nuestro estándar de vida retornaría, entonces, a niveles de subsistencia. Sostenía que estábamos condenados porque mientras la población tendía a crecer geométricamente, la producción de alimentos aumentaría sólo aritméticamente.

Durante 200 años los economistas han desestimado a Malthus porque no tuvo en cuenta los avances técnicos. Argumentan que la producción de comida puede, en efecto, crecer geométricamente porque la producción no sólo depende del suelo, sino también del conocimiento técnico. Con los avances en selección de semillas, abonos químicos, sistemas de riego y mecanización, las provisiones de alimentos pueden mantenerse muy por encima de la curva de población. En un sentido más amplio, los avances técnicos en todos sus aspectos pueden hacer que la producción de alimentos se mantenga por encima del crecimiento de la población. Tampoco parece que Malthus reparase en la transición demográfica: las mejoras de la salud pública, la planificación familiar y los métodos anticonceptivos que, junto con la urbanización y otras tendencias, pueden reducir espectacularmente la tasa de fertilidad hasta la "tasa de reemplazo" de 2,1 niños por familia, o incluso menos.

Cuando yo estudiaba economía, el razonamiento malthusiano era objeto de burla; mis profesores lo ponían como ejemplo de previsiones absolutamente erradas. Después de todo, desde los tiempos de Malthus la media de ingresos *per capita* en el mundo ha aumentado en al menos un orden de magnitud a pesar del aumento de población, que ha pasado de alrededor de 800 millones a 6700 en ese período. Algunos economistas han llegado incluso a sostener que, más que un impedimento, el crecimiento de la población ha sido una de las causas fundamentales de la mejora de la calidad de vida, porque, al multiplicarse por ocho, el número de genios ha aumentado proporcionalmente, y es la genialidad, sobre todo, lo que impulsa el avance de la humanidad en el mundo. Según esta interpretación, una población numerosa es precisamente lo que hace falta para impulsar el progreso.

Aun así, el fantasma de Malthus no se ha desvanecido. La mejora de nuestro conocimiento no sólo ha servido para sacar más provecho con el mismo esfuerzo, sino también para explotar la tierra con mayor eficiencia e intensidad. La humanidad ha aprendido a cavar más hondo en busca de minerales y combustibles fósiles, a faenar en los océanos con redes más poderosas, a desviar ríos con mayores diques y canales, y a talar bosques con equipos de deforestación más capaces. En un sinnúmero de aspectos no hemos conseguido más por menos sino más por más, a medida que convertíamos ricas reservas de capital natural en grandes explotaciones para nuestro consumo habitual.

Y aunque con la planificación familiar y la contracepción se ha conseguido una tasa de fertilidad baja en muchas partes del mundo, la tasa global se mantiene en 2,6, muy superior a la de reemplazo. La población mundial continúa creciendo en alrededor de 79 millones de personas al año, y el mayor incremento se da en los países más pobres. Según las previsiones de fertilidad media de la División de Población de la ONU, estamos en camino de llegar a los 9200 millones de personas para mediados de siglo.

Si, definitivamente, nos quedamos sin petróleo barato y escasean los alimentos, agotamos los acuíferos y destruimos la selva tropical que aún queda, esquilmamos los océanos y llenamos la atmósfera de gases de efecto invernadero que están empujando el clima terrestre hacia un calentamiento desbocado, con el nivel de los océanos en aumento, podríamos muy bien confirmar la maldición malthusiana.

Con todo, nada de esto sería inevitable si en el futuro las técnicas nos permitieran conservar el capital natural en vez de buscar modos cada vez más ingeniosos de agotarlo rápidamente. En las próximas décadas tendremos que realizar la conversión a la energía solar y a la energía nuclear segura; ambas ofrecen esencialmente un suministro de energía ilimitado. El conocimiento tendrá que conseguir automóviles de gran autonomía, una agricultura con un uso eficiente del agua y edificios ecológicos que recorten drásticamente el consumo de energía. Necesitamos repensar las dietas modernas y el diseño urbano para conseguir estilos de vida más saludables que además reduzcan el consumo. Y para que la población global se estabilice en alrededor de ocho mil millones, tendremos que ayudar a Africa y a otras regiones a acelerar su transición demográfica.

Es indudable que todavía no estamos en ese camino. Necesitaremos políticas nuevas para empujar a los mercados en esa dirección y promover los avances técnicos en el ahorro de recursos. Necesitaremos nuevas formas de hacer política que reconozcan la importancia de una estrategia de crecimiento sostenible y de la cooperación mundial. Pero esta cooperación habrá de llegar en un momento en que la escasez de recursos lime los niveles de vida en muchos lugares y erosione la estabilidad política.

¿Hemos derrotado a Malthus? Dos siglos después de su obra, aún no estamos seguros.

Jeffrey D. Sachs es director del Instituto de la Tierra de la Universidad de Columbia.

MATT COLLINS

Confituras y mermeladas

Azúcares, pectina y ácidos constituyen los ingredientes básicos para preparar conservas de frutas, verduras y flores

Pere Castells



Para los ingleses, una mermelada es una preparación de cítricos con azúcar; una confitura, la cocción azucarada de otras frutas. En España los perfiles semánticos de una y otra quedan más confusos. En el habla popular, las confituras incluyen trozos de fruta, no así las mermeladas. Pero, en rigor, la diferencia reside en la elaboración: en la confitura se cuece la fruta con almíbar y en la mermelada se cuece una mezcla macerada de fruta y azúcar.

La normativa alimentaria describe la confitura como una mezcla, con la consistencia gelificada apropiada, de azúcares y pulpa, puré de frutas o ambos, cuyo contenido en materia seca soluble (equivalente al contenido en azúcares) es igual o superior al 60 %. Por su parte, la mermelada se define como un producto preparado por cocción de frutas a las que se han incorporado azúcares hasta conseguir una consistencia semilíquida o espesa, cuyo contenido en materia seca soluble debe situarse entre el 40 y el 60 %. Así pues, es el contenido en azúcares el factor que delimita la frontera entre confituras y mermeladas.

En la opinión de Georgina Regàs, del Museo de la Confitura del Torrent en Gerona, el proceso de obtención de ambas conservas es prácticamente el mismo. Seguiremos su criterio y emplearemos indistintamente *confitura* o *mermelada*, en el sentido amplio del término. Pero no podemos adentrarnos en los secretos de las mermeladas sin referirnos antes al "triángulo mágico" que constituyen el azúcar, la pectina y los ácidos.

En la preparación de mermeladas suele utilizarse azúcar blanco cristalizado. Este hidrato de carbono corresponde a la sacarosa, un disacárido (cadenas de glucosa y fructosa). Pueden emplearse también azúcar negro de caña, miel u otros ingredientes azucarados, si bien alteran demasiado el sabor y oscurecen el producto final. La utilización de glucosa, fructosa, azúcar invertido u otros tipos de azúcares queda reservada a pasteleros expertos y a la industria alimentaria.

MUSEO DE LA CONFITURA DEL TORRENT, GERONA

La pectina es otro hidrato de carbono, un polisacárido muy ramificado. En solución acuosa forma geles (es un hidrocoloide), por lo que espesa la elaboración. La acción de la pectina en la elaboración de mermeladas está condicionada por la concentración de azúcar y la acidez. Para que el efecto gelificante sea óptimo, el *p*H debe situarse entre 3,2 y 3,8 y el contenido en azúcares debe ser superior al 40 %. Ese gelificante natural se encuentra en numerosas frutas: grosella (1,7 %), albaricoque (1 %), ciruela (0,9 %), manzana (0,6 %), fresa (0,5 %) y cereza (0,3 %).

La acidez de la mezcla está garantizada por los ácidos presentes (cítrico, tartárico y málico). La mayoría de las recetas ofrecen, pues, condiciones adecuadas para la acción de la pectina (aun así, suele añadirse zumo de limón para asegurar un *p*H ácido).

El primer paso consiste en escoger un buen producto. Lo lavaremos y pelaremos, reservando, si es necesario, la piel (puede interesarnos para la extracción de pectina). Si la fruta se oxida con facilidad (manzana, pera, melocotón, albaricoque, níspero, nectarina), incorporaremos un poco de zumo de limón al pelarla para evitarlo.

Añadimos luego el azúcar a razón de 500 gramos por cada kilogramo de fruta (cortada y pelada). La cantidad de azúcar añadido puede modificarse en función del contenido en azúcares de la fruta: en cerezas, peras, piñas y melones (que contienen alrededor de un 12 % de azúcares) reduciremos la cantidad de azúcar añadido; en fresas, frambuesas, limones y moras (que contienen no más del 7 % en azúcares) la aumentaremos. Otro factor a tener en cuenta es el grado de maduración de la fruta: cuanto más madura, mayor contenido en azúcares.

Una vez añadido el azúcar a la pulpa, dejaremos macerar la mezcla durante unas 12 horas. Se producirá entonces un fenómeno osmótico: para equilibrar concentraciones, el agua del interior de las células de la fruta saldrá hacia el exterior, formando un sirope con el azúcar.

Coceremos luego la mezcla a fuego lento, durante unos 15 minutos, para provocar la transmisión de aromas. Si queremos conservar parte de la fruta fresca, retiraremos algunos trozos (excepto en el caso de los cítricos). Confitaremos a fuego fuerte la pasta durante unos 5 minutos, tras los cuales añadiremos de nuevo la fruta reservada junto con zumo de limón.

La aparición de burbujas indica el final del proceso. Sin embargo, comprobaremos la terminación del mismo mediante la prueba del plato: al colocar un poco de mermelada en un plato e inclinarlo, debemos observar que la viscosidad de la preparación ha aumentado debido a la pectina; una consistencia demasiado líquida indicará que todavía no hemos llegado al punto óptimo.

Una vez finalizado el proceso, se coloca la mermelada en recipientes de cierre hermético y la pasteurizamos en una olla con agua en ebullición (baño María) durante 35 minutos. Si cuando llenamos el recipiente observamos burbujas de aire en la mezcla, añadiremos unas gotas de destilado (ron, ginebra, vodka), que eliminará las burbujas. Si persisten, podrían echar a perder la conservación de la mermelada. (El uso de alcohol no debe preocuparnos, pues se evapora rápidamente.)

Esta receta básica puede extenderse a mezclas de frutas, verduras y flores. Sin embargo, en estas últimas, al no contener pectina ni azúcares, habrá que introducir elementos que aporten pectina (piel de manzana, cítricos) y aumentar la cantidad de azúcar añadido.

Pere Castells es el responsable del departamento de investigación gastronómica y científica de la Fundación Alicia.

PRIVACIDAD GENETICA

Se necesitan leyes más rigurosas para evitar que las compañías de seguros y los empresarios discriminen a clientes y trabajadores en razón de los resultados de pruebas genéticas

Mark A. Rothstein

CONCEPTOS BASICOS

- Los análisis genéticos van a difundirse pronto y rápido. Añadirán a los historiales médicos datos que van a estar en el punto de mira. Conforme esos registros pasen al formato electrónico, será cada vez más fácil que personas ajenas examinen nuestros datos médicos.
- Si se abre el acceso a datos confidenciales, las compañías de seguros médicos y de vida podrían denegar prestaciones a un individuo con riesgo de sufrir una enfermedad complicada. Las empresas podrían despedir o rechazar a un trabajador para evitar una carga excesiva al seguro médico de la compañía.
- Las leyes actuales ofrecen, en el mejor de los casos, una protección muy pobre. Se necesita una legislación que otorgue mayor control a los individuos sobre sus propios datos, que limite la divulgación no autorizada y que penalice a los infractores.

Antaño, si la familia del lector tenía antecedentes de cáncer de colon, no le quedaba otra opción que esperar y temer que él acabara sufriéndolo. Hoy en día, en cambio, un análisis genético le permite saber si ha heredado una predisposición superior a la media de padecer la enfermedad. Y así, poder beneficiarse de un tratamiento preventivo. Un mayor conocimiento de los genes mejora la capacidad de prevención, tratamiento y curación.

Ante esas perspectivas, el entusiasmo se desató en el comienzo del Proyecto Genoma Humano en 1990. Un fervor que se vio atenuado conforme crecía la inquietud por proteger la privacidad de la información genética. Los análisis que revelaran la dotación génica de un individuo podrían avergonzarle o estigmatizarle. Las compañías de seguros podrían denegarle la cobertura sanitaria o aumentar la prima; los empresarios podrían no contratarle o despedirle. Al propio tiempo, los científicos y las autoridades sanitarias admitían que nunca podría acometerse la potencial mejora de la asistencia médica basada en estudios genéticos de grandes poblaciones, si la mayoría de la gente se negaba a participar por miedo a que los resultados pudieran ser usados en su contra.

El inquietante escenario que generaría la temida discriminación genética no se ha hecho realidad... todavía. A pesar de que el Proyecto Genoma Humano terminó en 2003, los análisis genéticos no se han generalizado y, por tanto, hay poca información que divulgar del historial médico de una persona. El análisis exhaustivo del genoma sigue resultando muy caro. Además, se carece de técnicas que permitan realizar exploraciones del genoma entero para riesgos que acechen a la salud.

La verdad es que, en los países ricos sobre todo, los análisis genéticos de múltiples enfermedades serán pronto rutinarios. Impulsadas por nuevas técnicas y descubrimientos, se están desarrollando pruebas más útiles y asequibles. La rápida transición del historial médico en papel al soporte electrónico facilitará el acceso a la información genética. Salvaguardar la privacidad genética resulta más complicado de lo que pueda parecer. Las leyes recientes (como la norteamericana Ley de No Discriminación por Información Genética de 2008) ofrece escasa protección. Antes de que los análisis se generalicen y los abusos aumenten, deberá reforzarse la legislación.

Información por doquier

Averiguar la mejor manera de asegurar la privacidad genética sería más sencillo si "información genética" y "enfermedades genéticas" fueran conceptos fáciles de definir. Pero no lo son. Las investigaciones demuestran que casi todas las enfermedades tienen un componente genético. La distinción entre información sobre salud genética y no genética se diluye. Con todo, los políticos han optado por dar una protección especial a la información genética. A efectos jurídicos, las definiciones más corrientes incluyen los resultados de los análisis genéticos de un individuo, los de su familia y el historial médico de todos. Las enfermedades de familia suelen tener un componente genético.

Los datos que encajan en esas categorías están aumentando a ojos vista. En el último decenio, la investigación genética y sus aplicaciones clínicas han pasado de centrarse en enfermedades asociadas a un solo gen (fibrosis quística y distrofia muscular) a enfermedades más frecuentes y complejas, caracterizadas por la interacción entre múltiples genes y factores ambientales (asma, cáncer, cardiopatías y diabetes). En la actualidad, se están utilizando más de 1500 pruebas genéticas; se hallan en fase de desarrollo varios centenares más. A medida que los análisis de ese tipo formen parte de la práctica médica habitual, incluida la asistencia primaria, la mayoría de los historiales médicos, si no todos, contendrán una proporción notable de información genética.

Los análisis del genoma entero podrían aumentar esa información, puesto que permiten hallar, dentro de una secuencia de cientos de miles de nucleótidos cambios génicos individuales asociados a una enfermedad concreta. Los científicos consideran prematuro en su mayoría utilizar esa técnica de manera rutinaria. No obstante, algunas compañías como 23andMe, en Mountain View, California, y deCODE Genetics, en Reykiavik, han comenzado a comercializar con una publicidad agresiva las exploraciones del genoma entero. Pese a carecer de licencia para operar como un laboratorio de análisis médico. De aquí a diez años, la secuenciación de un genoma, —la lectura de todos y cada uno de los tres millones de nucleótidos de un ADN humano— podría estar disponible por menos de mil dólares.

Por lo menos otros dos factores contribuirán a la ampliación de la información que contienen los historiales médicos. Por un lado, la aspiración hacia una medicina personalizada (tratamientos farmacológicos hechos a la medida de cada paciente para aumentar la eficacia y disminuir los efectos secundarios) favorece el desarrollo de instrumentos para analizar el genoma entero. Esos análisis "farmacogenómicos" son ya práctica corriente en la selección de fármacos y dosis para el tratamiento de ciertos cánceres. Por otro lado, la "toxicogenómica" (estudio de la respuesta de los individuos a las sustancias tóxicas en función de su genoma) está adquiriendo una mayor importancia en la evaluación de los riesgos para la salud de



un individuo en el lugar de trabajo y en el ambiente en general.

Multiplicación de riesgos

Cada vez dependemos más de la información digital. Ello supone un desafío para la protección de datos médicos. Basados hasta ahora en un sistema de archivo en papel, las historias clínicas se están transformando en historiales médicos electrónicos (HME), lo que debería redundar en una mejora de la asistencia y una reducción de los costes. Dicha transición se ha iniciado ya en numeroso países desarrollados. En EE.UU., una red nacional de información de la salud (NIHN, de "Nationwide Health Information Network") se está elaborando a modo de "red de redes". Se propone establecer formatos electrónicos que harán compatibles documentos de todas clases, fáciles de transportar a través de la red y del país.

El HME de un individuo incluirá, pues, su historia clínica completa, "de la cuna a la tumba". La oficina del coordinador nacional para la Tecnología de la Información de la Salud, del departamento estadounidense de Salud y Servicios Humanos, dirige el desarrollo de la NIHN. Las administraciones estatales y el sector privado se han comprometido en la investigación, el desarrollo y la puesta en marcha de las pruebas.

La NIHN pone sobre la mesa asuntos polémicos. En un sistema en soporte de papel, la privacidad está protegida sobre todo por el caos. En razón del carácter fragmentario del sistema, resulta imposible recopilar o incluso localizar los documentos de un individuo, generados en múltiples servicios médicos de sitios distintos y a lo largo de muchos años. Mas un archivo exhaustivo y lineal contendrá, quiérase o no, información delicada. El paciente no podrá refugiarse tras el "recuerdo selectivo" de ciertos hechos al describir su situación al médico, ni podrá procurarse el servicio de un profesional sin el conocimiento de otro. A diferencia de lo que sucede en la actualidad, un diagnóstico antiguo de depresión hecho en una clínica mental o los resultados de un análisis genético realizado a raíz de una enfermedad familiar acabarán siendo una información permanente en un HME.

Un individuo con un trastorno que pudiera estigmatizarle (toxicomanía, por ejemplo), podría retrasar o anular un tratamiento. Ello resultaría desastroso para él y para la sanidad pública. No obstante, no se necesita disponer de un historial completo para ofrecer una asistencia médica eficaz. Un médico que trata un esguince de tobillo no necesita saber si un paciente tiene predisposición a sufrir cáncer de mama, ni un dentista que pone un empaste enterarse de si hay antecedentes familiares de la enfermedad de Huntington.

Para proteger a las personas de la divulgación innecesaria de información confidencial, ciertos países (Canadá, Holanda y el Reino Unido) están considerando estrategias que permiten limitar la información revelada en función del profesional sanitario que la recibe. Esas medidas incluyen dar al paciente un control completo de su historial médico, permitiéndole eliminar información antigua y limitarla a los detalles necesarios para un diagnóstico determinado o según el tipo de profesional. Se aplicarían reglas especiales para retener la información más delicada mediante la creación de un subconjunto de datos de salud básicos que estarían disponibles para todos los profesionales. Asimismo, se crearían bancos de historiales médicos independientes, que divulgarían los documentos según lo indicado por el paciente. En la red de HME danesa, una de las más avanzadas, los individuos pueden "bloquear" cualquier información de su registro. Aunque esa opción no suele utilizarse, está muy valorada.

En EE.UU. no existen ese tipo de cautelas. En febrero de este año, la Comisión Nacional de Estadística Demográfica y Sanitaria, que asesora al secretario de salud y servicios humanos, recomendaba que los individuos

CURIOSOS PERO DESCONFIADOS

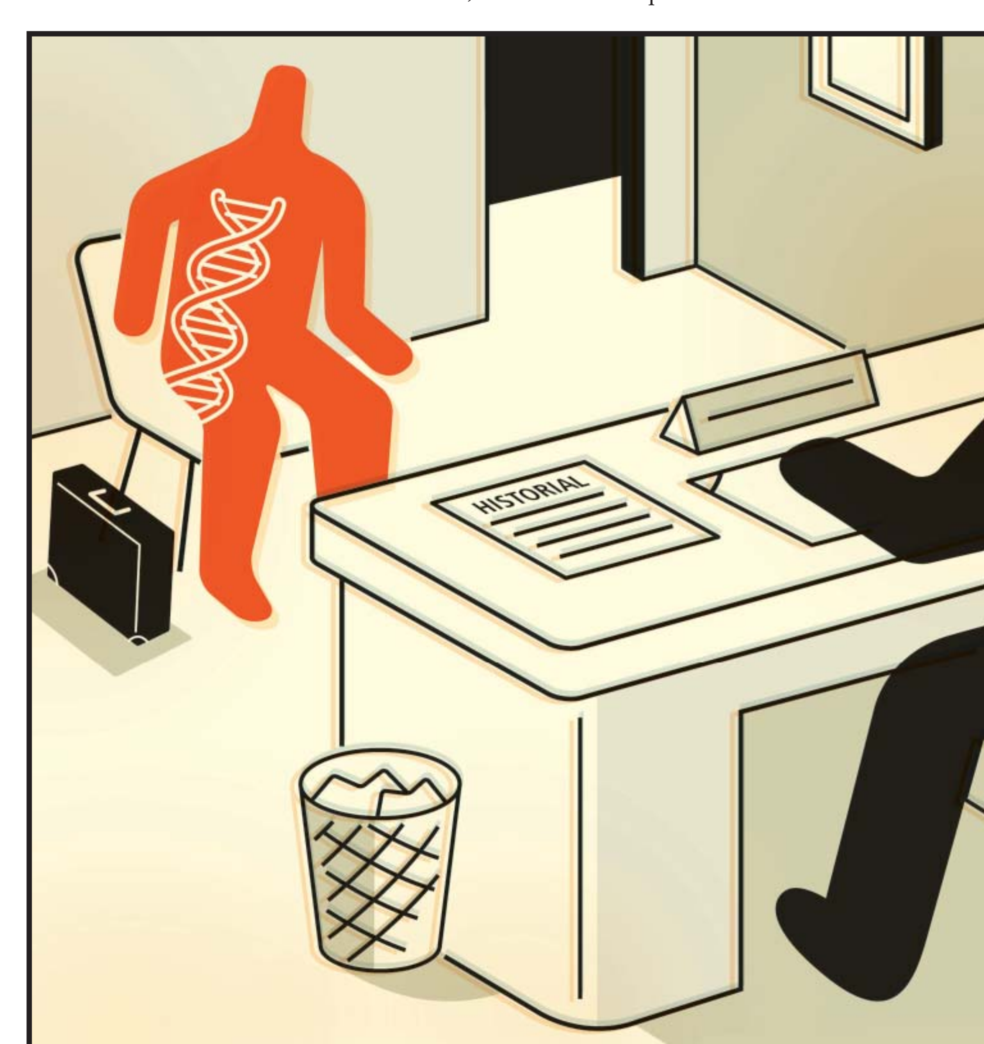
Según una encuesta realizada en mayo de 2008 por la compañía Knowledge Networks:

El 47 por ciento de los estadounidenses están interesados en usar los servicios en línea de archivos de sus historiales médicos tales como Google Health o Microsoft HealthVault. Esos servicios permiten a los usuarios controlar en línea su propio historial.

Sin embargo, el 90 por ciento de los encuestados recelan de la capacidad de dichos servicios para mantener la confidencialidad de los historiales médicos.

La fundación Markle recomienda varios medios para mejorar la privacidad de los sistemas. Ciertas cláusulas permitirían a los usuarios verificar quién accede a sus datos y cuestionar la información proporcionada por los profesionales sanitarios.

HARRY CAMPBELL



pudieran impedir la divulgación rutinaria de la información sanitaria confidencial en categorías predefinidas: violencia doméstica, drogadicción, salud mental, enfermedades de transmisión sexual e información genética. Pero los métodos para poner en práctica tales recomendaciones no se han desarrollado todavía. Es más, seguimos sin esclarecer el modo de alcanzar el equilibrio entre una divulgación amplia y restringida. Si el paciente goza de un control desmesurado, los médicos no tendrán confianza en la exactitud o completitud de su historial. Como consecuencia, es probable que soliciten nuevas pruebas, lo que debilitará la eficacia de la red y añadirá gastos. Por el contrario, si el paciente tiene poco control, quizá tome medidas defensivas: no entrar en la red, pagar tratamientos extraoficiales en efectivo o renunciar a cierto tipo de asistencia.

Y otras cuestiones quedan pendientes. ¿Deberían aplicarse las reglas de confidencialidad a sistemas que analizan registros electrónicos y notifican a los médicos una posible interacción farmacológica, de manera que el sistema no divulgue la medicación tomada? ¿Debería indicarse al personal sanitario que cierta información del historial clínico no está disponible a petición del paciente? ¿Pueden los médicos acceder a la información restringida en caso de que la persona necesite asistencia urgente?

Leyes débiles

Con más información genética y redes electrónicas de largo alcance en el horizonte, una legislación que proteja la privacidad clínica resulta esencial. Por desgracia, en EE.UU. no existen leyes de alcance general. Lo más cercano a una salvaguardia nacional es la Ley de Responsabilidad y Transferencia de Seguros Médicos (HIPAA, de “Health Insurance Portability and Accountability Act”) de 1996 y su Reglamento de Privacidad añadido en 2003. El Reglamento de Privacidad expone de forma detallada los casos lícitos de uso y divulgación de la información clínica por parte de profesionales sanitarios, planes de salud y bases de datos que gestionan la compensación de gastos médicos.

Con todo, existe una gran laguna jurídica. El Reglamento de Privacidad se aplica sólo a las entidades que manejan de forma electrónica los datos de reclamaciones médicas. Pero cientos de miles de establecimientos y profesionales no lo hacen todavía: médicos que cobran sólo en efectivo, gimnasios que piden información médica antes de planificar un entrenamiento y profesionales sanitarios que trabajan a cuenta de terceros (personal contratado en clínicas locales). Un problema asociado es la no aplicación de la ley. Unas



DAVID ELLIS

¿Debo decírselo a mi familia?

Sara tiene 40 años y es madre de tres niños. Tras realizar varias pruebas ha descubierto que tiene una gran probabilidad de padecer la enfermedad de Alzheimer y cáncer de mama. ¿Tiene la obligación legal o moral de decirles a sus hijos y parientes más próximos que también ellos podrían correr un riesgo elevado de sufrir las mismas enfermedades?

Desde el punto de vista legal está claro: ningún tribunal ha considerado un individuo responsable de no prevenir a un pariente sobre los resultados de una prueba genética. La cuestión moral, en cambio, depende de varios factores: la gravedad del trastorno genético, el número de años que quedan hasta la probable aparición de los síntomas y la posibilidad de tratamiento. También cuenta la naturaleza del parentesco (padres e hijos) y su cercanía emocional, así como la edad de los familiares, su interés en conocer la posibilidad de enfermedades futuras y la preocupación del individuo por no divulgar sus problemas personales.

La naturaleza del peligro importa también. Y mucho. En casos raros, una enfermedad genética resulta letal si se combina con factores ambientales desencadenantes. Por ejemplo, individuos con la mutación génica para la hipertermia maligna pueden morir durante una operación si se utiliza cierto tipo de anestesia. Las personas con miocardiopatía hipertrófica pueden morir de forma súbita tras realizar ejercicio intenso. Ante el peligro que entraña ese tipo de enfermedades, parece más que justificado prevenir a los parientes del riesgo que pueden correr.

Sin embargo, compartir la información genética con miembros de la familia puede resultar peligroso. Los análisis pueden revelar, por ejemplo, que el marido que todos pensaban que era el padre biológico del niño no lo es. Los asesores genéticos ayudan a las personas a decidir si se someten a un análisis genético y a afrontar los resultados. Sin embargo, en los EE.UU. ejercen sólo 2500 asesores. El error más frecuente es realizar el análisis y no tomar ninguna decisión hasta que no se conocen los resultados. Cualquier persona que piense en realizar las pruebas genéticas debe antes considerar si va a hacer partícipe a su familia más cercana. La respuesta no es fácil. El mejor consejo es consultar a profesionales y prevenir las posibles consecuencias.

36.000 quejas relacionadas con el Reglamento de Privacidad llegaron al despacho de derechos civiles del departamento de Salud y Servicios Humanos entre abril de 2003 y mayo de 2008. Aunque se han hecho algunas rectificaciones, se ha evaluado sólo una multa civil hasta la fecha. No hay suficientes medidas disuasorias para los infractores.

Además, la HIPAA es de cumplimiento obligado sólo para las entidades involucradas en la atención sanitaria. Al ciudadano de a pie, sin embargo, le preocupan más el estigma o la discriminación que pueda sufrir. Tiene miedo de las complicaciones que pueden surgir cuando solicite un trabajo, quiera contratar un seguro de vida o beneficiarse de una indemnización laboral. Todavía es frecuente exigir al

usuario un consentimiento firmado para que sus médicos expidan el historial clínico. Se estima que en Estados Unidos se firman cada año unos 25 millones de esas autorizaciones.

Las partes que requieren la cesión de los datos suelen actuar conforme a la ley. Es lícito que una empresa se interese por la salud de un trabajador y su aptitud para realizar una tarea concreta. Una compañía eléctrica, por ejemplo, no querría contratar a una persona propensa a sufrir ataques de epilepsia para subir a reparar los cables de un poste de electricidad. El problema es la cantidad de información revelada. La compañía eléctrica no necesita saber si su candidato tiene una mutación genética que puede aumentar el riesgo de sufrir una enfermedad cardiaca dentro de varios decenios. Si un trabajador solicita indemnización laboral por un traumatismo, los evaluadores no necesitan ningún informe sobre su salud reproductiva. Un perito de un seguro automovilístico que estudia una indemnización por un diente roto en un accidente no necesita ningún análisis genético. No obstante, la mayoría de las leyes que autorizan la divulgación de la información médica están escritas en líneas tan generales, que no imponen ningún límite al alcance de las peticiones.

La paradoja es que las redes de HME resolverían este problema. Los programas informáticos podrían analizar los registros electrónicos y seleccionar sólo los datos relacionados con una cuestión concreta. Con todo, esta posibilidad requiere la aplicación de criterios de acceso contextual, algoritmos que especifican que, para una pregunta de tipo X, se necesitan sólo los datos A, B y C. Por ejemplo, los criterios de acceso contextual divulgarían a una compañía de seguros de vida sólo la información relacionada con el riesgo de mortalidad. Esa técnica es factible, pero aún no está disponible. Puesto que es probable que la demanda comercial no garantice por sí sola los incentivos necesarios para desarrollar la técnica, va a ser necesario que las leyes lo exijan.

Magro apoyo legal

Dada la debilidad general de las leyes federales, varios estados han promulgado sus propias leyes de protección, basadas en la noción de "excepcionalismo genético" (la información genética recibe un trato distinto del de otro tipo de información confidencial). No sabemos todavía si ese enfoque es el adecuado, pero guarda analogía con el trato que reciben las enfermedades mentales, la toxicomanía y la información sobre VIH.

A pesar de que cada estado tiene sus propias leyes, 12 de ellos piden a los ciudadanos dar un consentimiento informado por escrito para hacerles una prueba genética; 27 requieren el consentimiento expreso para comunicar los resultados de las pruebas. Sin embargo, esas leyes, lo mismo que las federales, siguen permitiendo que las aseguradoras y los empresarios exijan a las personas firmar una autorización para la cesión de sus datos médicos. En respuesta, 47 estados prohíben a las compañías de seguros denegar o restringir las prestaciones, así como aplicar tarifas distintas en función del perfil génico del cliente. La HIPAA cubre esos casos para las personas con planes de salud colectivos promocionados por empresas, de modo que las leyes estatales ofrecen protección sólo a quienes han contratado un seguro individual.

En 35 estados, otras leyes prohíben a las empresas exigir una prueba genética como requisito para obtener un empleo o utilizar una información genética con capacidad predictiva para rechazar a un individuo en un trabajo. Sin embargo, tras una oferta de empleo, las leyes permiten que las empresas requieran el consentimiento de sus futuros empleados para acceder a su historial médico como condición para ser contratados. Los estados discrepan sobre si la información genética puede divulgarse en este momento, pero esta disposición es en gran medida irrelevante ya que resulta imposible eliminar la información genética de registros en papel o excluir dicha información de los archivos electrónicos, a menos que se disponga de un algoritmo de acceso contextual.

A la vista de tales deficiencias, el congreso está sometido a una presión creciente para mejorar la privacidad. En mayo, se aprobó por fin la Ley de No Discriminación por Información Genética (GINA, de "Genetic Information Non Discrimination Act"), que estaba pendiente desde mediados de los años noventa. La ley prohíbe a las compañías de seguros la discriminación, según la predisposición genética, en la concesión de prestaciones y la aplicación de tarifas. Por desgracia, la legislación federal no es mejor o ni siquiera distinta de muchas leyes estatales: no cubre seguros de vida, de invalidez ni de asistencia médica a largo plazo.

Soluciones universales

Los defectos de la GINA, de la HIPAA y de las normas estatales no corresponden a lagunas jurídicas o descuidos. Son el resultado natural de un sistema sanitario privado (la asistencia médica de cada individuo está cubierta por compañías de seguros). En EE.UU., los individuos pueden contratar un seguro médico mediante una de estas tres formas: un plan de salud colectivo (como los que ofrecen la mayoría de las empresas), un seguro individual o un programa federal (Medicare y Medicaid).

EL GENOMA AL DETALLE

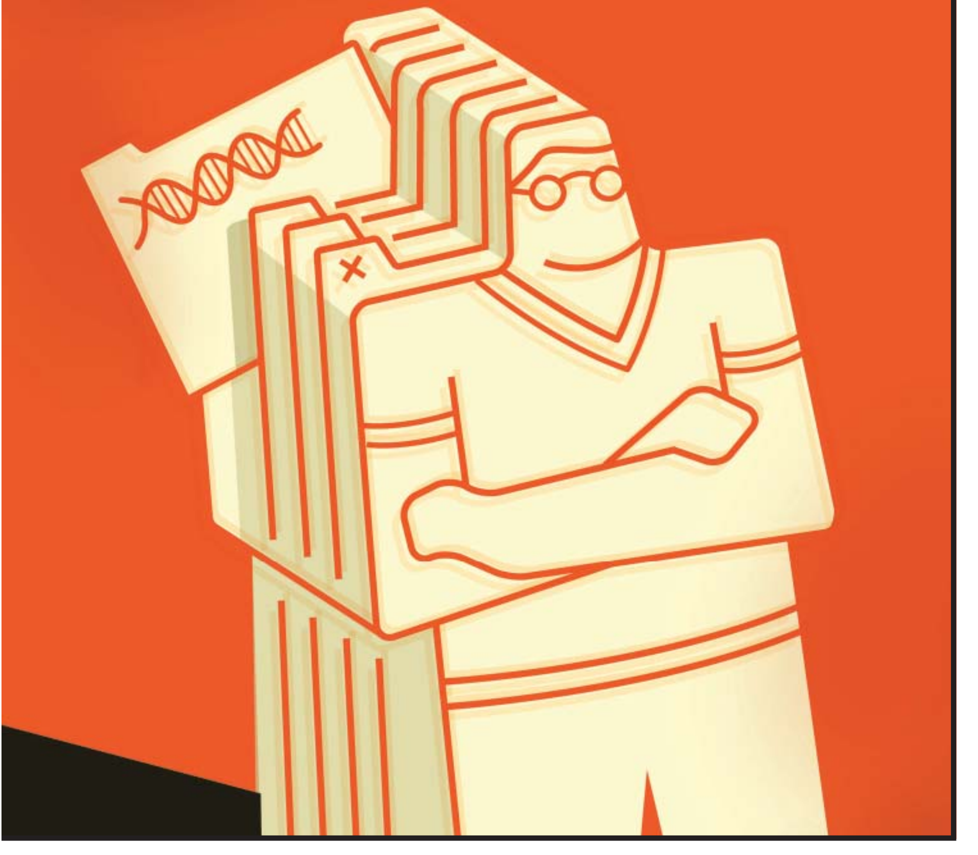
El Proyecto Genoma 1000, un consorcio de investigación internacional establecido en 2008, se propone crear un mapa del genoma humano cinco veces más detallado que el obtenido por el Proyecto Internacional Hapmap.

Los descubrimientos del Hapmap generaron la reciente explosión de estudios del genoma entero. Se han descubierto más de 130 variantes génicas asociadas a enfermedades: diabetes de tipo 2, cardiopatía coronaria, cánceres de mama y próstata, artritis reumatoide y ciertos trastornos mentales.

En los tres próximos años, el Proyecto Genoma 1000 espera secuenciar el genoma de al menos 1000 personas de todo el mundo. Para más información véase www.1000genomes.org

El autor

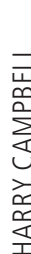
Mark A. Rothstein es catedrático de derecho y medicina, y director del Instituto de Bioética, Salud, Política y Derecho de la facultad de medicina de la Universidad de Louisville. De 2001 a 2008 dirigió el subcomité de Privacidad y Confidencialidad de la Comisión Nacional de Estadística Demográfica y Sanitaria que asesora a la secretaría estadounidense de salud y servicios humanos.



Para los planes colectivos e individuales, los agentes de seguros calculan los riesgos sanitarios individuales y colectivos de los asegurados e imponen primas basadas en el riesgo relativo que representan. Por supuesto, el principal objetivo es proteger los intereses financieros de las compañías aseguradoras. Estas quieren conocer las patologías del pasado y las posibles enfermedades futuras (genéticas o no), de manera que puedan determinar mejor el precio y rechazar a los solicitantes que en un futuro pudieran reclamar indemnizaciones astronómicas.

Ninguna de las leyes de confidencialidad mencionadas se aplica a Medicare o Medicaid, porque técnicamente corresponden a derechos, no a seguros. Algunas leyes tratan de proteger la información dentro de esos programas, pero el gobierno carece de un incentivo real para examinar la información genética de nadie, pues no hay tarifas que ajustar.

Los problemas para mantener la confidencialidad de la información están mejor resueltos en Canadá, donde existe un sistema público de asistencia sanitaria universal. En los planes universales, el riesgo se distribuye entre toda la población, que es a su vez quien los financia. El que una persona determinada presente un alto riesgo de padecer cierta enfermedad no influye en la ecuación, por lo que no hay ninguna razón para que otros traten de recabar información confidencial. Esta situación elimina las dos principales preocupaciones del ciudadano: tener problemas en la contratación de un seguro médico y ser rechazado en un trabajo porque su riesgo de enfermar impone una carga excesiva al plan médico de la compañía.



Bibliografía complementaria

GENETIC PRIVACY: A CHALLENGE TO MEDICO-LEGAL NORMS. Graeme Laurie. Cambridge University Press, 2002.

GENETIC PRIVACY. Pamela Sankar en *Annual Review of Medicine*, vol. 54, págs. 393-407; 2003.

GENETIC EXCEPTIONALISM AND LEGISLATIVE PRAGMATISM. Mark A. Rothstein en *Hastings Center Report*, vol. 35, n.º 4, págs 27-33; julio/agosto, 2005.

ENSURING THE PRIVACY AND CONFIDENTIALITY OF ELECTRONIC HEALTH RECORDS. Nicolas P. Terry y Leslie P. Francis en *University of Illinois Law Review*, págs. 681-735; 2007.

La contratación de un seguro de vida entraña todavía ciertas complicaciones. La confidencialidad de la información sanitaria debe asegurarse, para que los datos no puedan robarse ni divulgarse de forma incorrecta. Con todo, las mayores causas de discriminación desaparecen.

No obstante, es improbable que EE.UU. adopte pronto un sistema de asistencia sanitaria universal, aunque figure entre las prioridades de los discursos electorales. Por tanto, deben promulgarse mejores leyes de privacidad, aunque algunos observadores afirmen que las nuevas técnicas genéticas suponen sólo una pequeña amenaza para la privacidad.

Han llegado a los tribunales muy pocos pleitos sobre discriminación laboral o contratación de seguros. Pese a ello, genetistas y asesores saben de numerosos pacientes que han rehusado hacerse un análisis genético por miedo a ser discriminados o estigmatizados. (Según Francis S. Collins, antiguo director del Instituto Nacional de Investigación del Genoma Humano, una tercera parte de la gente cualificada para participar en una investigación genética rehúsa participar por miedo a la discriminación.) Además, el número de pruebas genéticas y de individuos que se someterán a éstas, junto con la utilidad de las mismas, aumentará en el próximo decenio. Las redes de HME facilitarán, mediante un solo clic, la divulgación de la información.

Mientras EE.UU. y otros países estudian mejores vías para el tratamiento de la información genética, los políticos se van percatando de que la protección de la privacidad no es tarea fácil ni barata. Es necesario mejorar las medidas de seguridad para impedir que la información se divulgue sin autorización; hay que limitar la trascendencia de las divulgaciones autorizadas. Resulta esencial —y todo un reto— decidir qué individuos y entidades tienen derecho a qué datos y con qué fines.

Una legislación efectiva debería, como mínimo, incluir cuatro directrices. Primera, abordar las dificultades para acceder a un seguro médico y equilibrar los derechos de empresarios y trabajadores. Segunda, limitar los usos extramédicos de la información sanitaria con capacidad predictiva, incluidos los seguros de vida, el seguro de discapacidad y el seguro de asistencia médica a largo plazo. Tercera, limitar el alcance de los datos divulgados, penalizar a los transgresores y proporcionar soluciones a los perjudicados. Y cuarta, las redes de HME y los HME deben diseñarse de manera que puedan limitar la divulgación de información sanitaria relevante. El plantearse tales cuestiones supone ya un primer paso para configurar el futuro de la privacidad médica.



INSTRUMENTOS DE ESPIONAJE

Las cámaras de visión nocturna, los sensores biométricos y otros artilugios permiten ya fisgonear en espacios privados. Pronto aparecerán unos "insectos robot" que caben en la palma de la mano

Compilado por Steven Ashley



Medios visuales

1 **LAS CAMARAS DIGITALES FOTOGRAFICAS Y DE VIDEO** equipadas con grandes lentes de teleobjetivo permiten distinguir los detalles de una escena lejana. Armados de una cámara con teleobjetivo se pueden leer los titulares (y quizá los subtítulos) de un periódico de un extremo a otro de un campo de fútbol.

2 **LOS ANTEOJOS DE VISION NOCTURNA** o los telescopios provistos de tubos fotomultiplicadores aumentan espectacularmente el brillo de la luz existente; hay sensores térmicos que descubren, por el calor, cuerpos y motores en oscuridad total.

Identificadores biométricos

3 **LA VOZ**, los rasgos faciales, la forma de andar y otras características permiten identificar una persona con particularidades físicas o de conducta que estén registradas en una base de datos.

4 **EL SENSOR DE ADN**, uno de los sistemas biométricos más recientes, toma muestras de ADN de un vaso o picaporte y las compara con la información genética de un archivo.

5 **LA NARIZ ARTIFICIAL** detecta la "huella olfativa corporal" de una persona y la coteja con las que haya registradas.

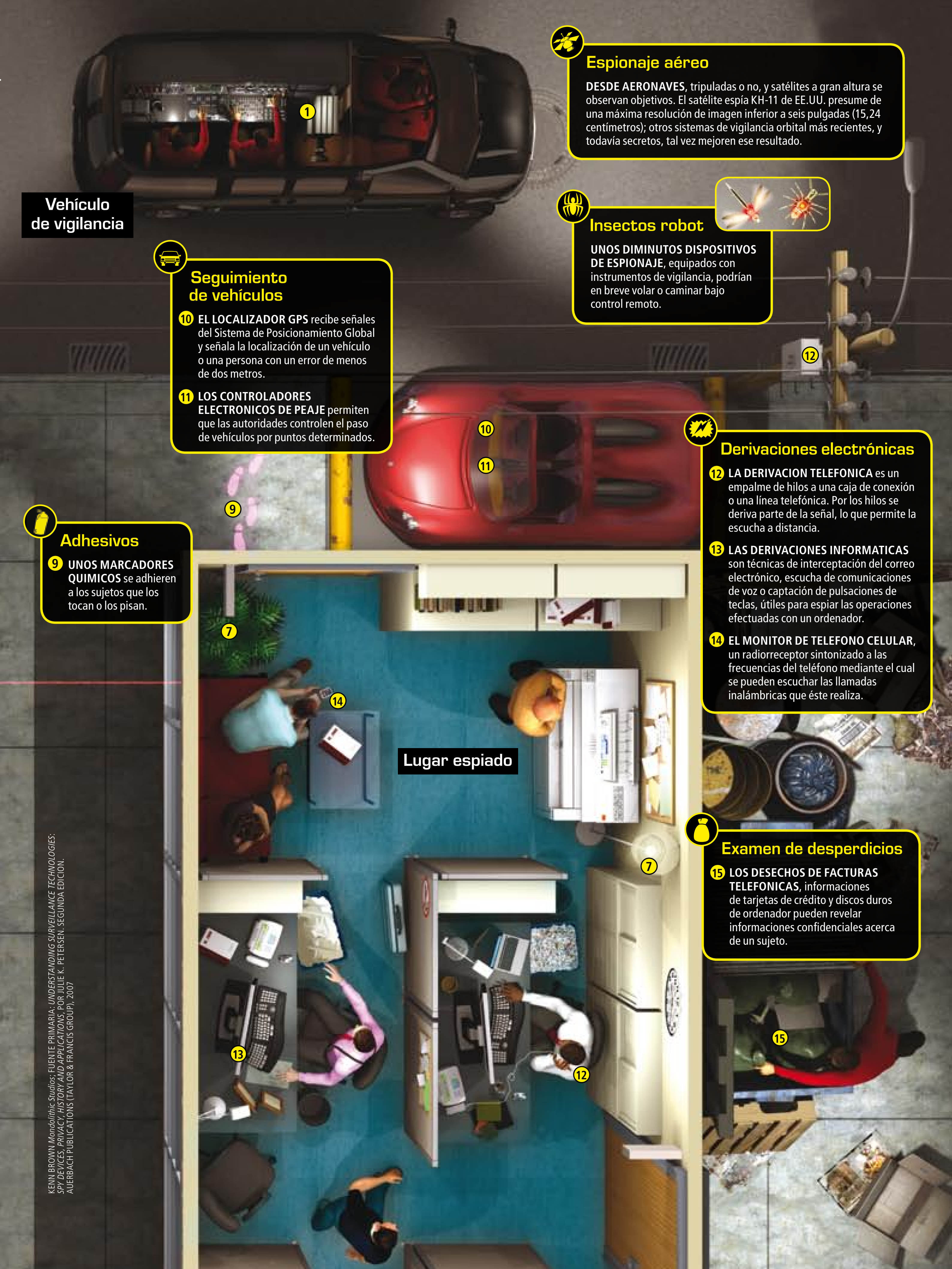
Dispositivos de escucha

6 **EL MICROFONO DIRECCIONAL**, asistido por un reflector parabólico o una "escopeta" (varilla lineal), puede captar conversaciones al aire libre a cien metros de distancia.

7 **UN MICROFONO OCULTO DIMINUTO** con radiotransmisor de corto alcance (*por ejemplo, dentro del tiesto de la página siguiente*), envía conversaciones a un radiorreceptor que las retransmite a una grabadora o unos auriculares (*agente sentado, abajo*).

8 **EL LASER** fijado al exterior de una ventana detecta vibraciones del vidrio producidas por los sonidos de conversaciones interiores. Un receptor óptico convierte las variaciones del haz reflejado en sonidos audibles.

Lugar de vigilancia

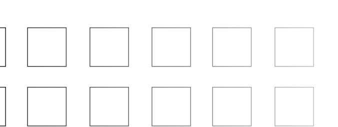


KENN BROWN *Mondolithic Studios*; FUENTE PRIMARIA: *UNDERSTANDING SURVEILLANCE TECHNOLOGIES: SPY DEVICES, PRIVACY, HISTORY AND APPLICATIONS*, POR JULIE K. PETERSEN. SEGUNDA EDICION. AUERBACH PUBLICATIONS (TAYLOR & FRANCIS GROUP), 2007

ETIQUETAS PERSONALES DE RFID

Las minúsculas etiquetas de identificación por radiofrecuencia, largo tiempo utilizadas para el control de existencias e inventarios, se engastan ahora en numerosos artículos de consumo. Ello plantea nuevos riesgos para la privacidad

Katherine Albrecht



CONCEPTOS BASICOS

- Las etiquetas de identificación por radiofrecuencia (RFID) se incorporan a un número creciente de efectos personales y documentos de identidad.
- Dado que estas etiquetas se diseñaron para el seguimiento y ofrecen escasa seguridad, quien las porte se expone a ser vigilado y seguido de un modo subrepticio.
- A escala mundial se ha prestado escasa atención legal a la protección del ciudadano frente a tales intromisiones.

Los residentes en un estado fronterizo con Canadá o México quizá muy pronto puedan emplear un artículo de técnica avanzada: un permiso de conducir legible a distancia. El Departamento de Seguridad Nacional de EE.UU. promueve el uso de una tarjeta diseñada para identificar a los ciudadanos que se acercan a los límites del país, evitando así dilaciones y molestias al cruzar la frontera. Ahora bien, si, amén de la comodidad, nos preocupa nuestra intimidad y seguridad, los estadounidenses deberían pensarlo dos veces antes de solicitar ese nuevo carné de conducir.

Los nuevos permisos estarán equipados con etiquetas de identificación por radiofrecuencia (RFID), que podrán ser leídas a través del bolsillo, la cartera o el bolso, a distancias de hasta 9 metros. Cada etiqueta incorpora un microchip codificado con un número de identificación exclusivo. Al aproximarse el portador a un puesto fronterizo, una antena conectada al chip capta la energía radiada por el dispositivo lector de dicho puesto y provoca la emisión del número de identificación (ID). Cuando el titular del permiso llega a la frontera, ese ID ha entrado ya en una base de datos del departamento de Seguridad Nacional; el agente visualiza en su pantalla la fotografía del viajero y otros datos de interés.

Aunque esos permisos de conducir de última generación son de uso voluntario en los estados que los ofrecen, los expertos en seguridad y privacidad temen que los usuarios de los nuevos carnés desconozcan los riesgos a que se exponen: *cualquiera* que posea un dispositivo lector (comerciantes sin escrúpulos, agentes del gobierno, espías, ladrones o, simplemente, entrometidos, cualquiera puede conseguirlo fácilmente), tendrá también acceso a los datos que figuren en el permiso de conducir, con lo que podrá vigilar desde lejos a su dueño, sin el conocimiento ni consentimiento del mismo.

Y no sólo eso, una vez que el número ID se ha asociado a una identidad individual (por ejemplo, cuando el portador del permiso efectúa una transacción mediante tarjeta de crédito), la etiqueta de radiofrecuencia adquiere un poder delegado por esa persona.

Los permisos de conducir se convertirán, pues, en la última incorporación en una serie interminable de artículos "etiquetados" que los consumidores podrían vestir o llevar consigo: abonos de transporte, pases de peaje, tarjetas de acceso a la empresa, carnés de estudiante, tarjetas de crédito "sin contacto", ropa, teléfonos e incluso artículos alimenticios.

Las etiquetas RFID se han asimilado a códigos de barras que radian su información. La comparación es oportuna por cuanto estos minúsculos dispositivos han servido sobre todo para identificar e inventariar piezas a medida que recorren cadenas de distribución. En vez de tener que escanear el CUP (código universal de producto) de cada artículo por separado, el almacenero registra el contenido de toda una plataforma de paquetes de rollos de papel de cocina, por ejemplo, mediante la

MELISSA THOMAS (*fotoilustración*); RICHARD SCHULTZ (*etiquetas RFID*); SAM JORDASH (*mujer*); BURAZIN (*llavero*); © 2005 TRANPORT FOR LONDON (*tarjeta Oyster*); IDENTITY STRONGHOLD (*funda de pasaporte*); DIMA GAVRYSH *AP Photo* (*tarjeta de crédito Chase blink*); ROLF VENNENBERND *DPA/Corbis* (*EAS/RFID*); WASHINGTON METROPOLITAN AREA TRANSIT AUTHORITY (*tarjeta SmarTrip*)



lectura del número de serie exclusivo codificado en la etiqueta RFID adjunta. Número que se asocia, en una base de datos centralizada, a una lista detallada del contenido del palé.

Pero las personas no somos meros objetos. En el último decenio se ha registrado una tendencia a incorporar chips en bienes de consumo individuales. Ahora, los documentos de identidad oficiales han creado un nuevo repertorio de problemas de privacidad y seguridad, precisamente por la enorme capacidad de seguimiento de la identificación por radiofrecuencia. Las propias etiquetas adolecen de falta de seguridad; las leyes actuales ofrecen escasa protección contra una intromisión subrepticia en un mundo cada vez más sujeto a control.

Más allá del código de barras

Las primeras etiquetas de radiofrecuencia sirvieron para identificar como amigos o enemigos a los aviones militares durante la Segunda Guerra Mundial. A finales de los años ochenta del siglo pasado, unas etiquetas similares se convirtieron en la base de los sistemas de pago electrónico de peaje (E-ZPass, en la costa este estadounidense). En 1999 empezaron a considerarse las posibilidades que ofrecían las etiquetas para el seguimiento de millones de objetos individuales. Aquel mismo año, Procter & Gamble y Gillette (unidas desde entonces para convertirse en el mayor fabricante mundial de productos de consumo) formaron un consorcio con ingenieros del Instituto de Tecnología de Massachusetts, el Centro Auto-ID. Su objetivo era desarrollar etiquetas de identificación por radiofrecuencia pequeñas, eficaces y suficientemente baratas para llegar a reemplazar los códigos de barras CUP en los productos de consumo cotidiano.

Hacia 2003, el grupo había desarrollado una primera versión de la técnica, que atrajo

LOS CONSUMIDORES tal vez no se percaten de las numerosas etiquetas de RFID que llevan encima. Estos chips se hallan incrustados en artículos personales y hasta en prendas de vestir.

inversiones de más de 100 compañías y organismos gubernamentales. Los promotores de las etiquetas prometieron que esos diminutos chips revolucionarían la gestión de los inventarios y evitarían las falsificaciones [*véase* “Sistemas de identificación por radiofrecuencia”, Roy Want, Investigación y Ciencia, marzo de 2004].

Para imprimir rapidez a la adopción de la técnica, la Administración General de Servicios estadounidense (entidad federal que gestiona las compras de otras instituciones oficiales) emitió en 2004 un memorándum en el que instaba a todos los jefes de agencias federales a “considerar actuaciones que hagan progresar la industria [de RFID]”. Repentinamente, casi todas las agencias, de la Administración de la Seguridad Social a la de Alimentos y Fármacos, empezaron a anunciar pruebas de la RFID.

Durante ese mismo período, se desarrollaron iniciativas similares en todo el mundo. En 2003, la Organización de Aviación Civil Internacional (OACI), agencia de las Naciones Unidas que establece normas mundiales para los pasaportes, apoyó el uso de etiquetas RFID en estos documentos. La OACI propugna hoy el empleo de las mismas en todos los pasaportes electrónicos; hay ya docenas de países, entre ellos EE.UU., que expiden tales pasaportes con etiquetas RFID insertadas.

Desde su debut, los nuevos pasaportes han sido tema de controversia, en cuanto a privacidad y seguridad. En 2006, un comunicado de la OACI prometía que las medidas de cifrado aplicadas tranquilizarían al más desconfiado titular de pasaporte: nadie podría leer sus datos personales sin su conocimiento.

Los expertos en seguridad no tardaron en demostrar lo contrario. En 2007, Adam Lauric, consultor de seguridad, descifró el código de un pasaporte del Reino Unido y leyó a distancia la información personal que contenía, pese a estar sellado y dentro de un sobre. Por esas mismas fechas, Lukas Grunwald, otro consultor, copió los datos del chip insertado en un pasaporte alemán y los codificó en una etiqueta RFID distinta para crear un documento falso que pudiera engañar a un lector de pasaportes electrónicos. Un equipo de investigadores de la Universidad Carolina de Praga encontraron análogos puntos flacos en los pasaportes electrónicos checos. Una técnica diseñada para eliminar los ataques a la seguridad en realidad los estaba estimulando.

Pese a todo, esos notorios fallos de seguridad no han retrasado la adopción de la identificación por radiofrecuencia. Antes bien, las tarjetas de identificación de uso doméstico se extienden por todo el mundo. Malasia ha expedido unos 25 millones de carnés nacionales de identidad que operan “sin contacto” (por proximidad). Qatar está preparando un carné que, además de la información personal, contiene la huella dactilar del titular. El gobierno chino ha invertido el equivalente a 4000 millones de euros en el proyecto de RFID más ambicioso del mundo: implantar la RFID en el documento nacional de identidad de casi mil millones de ciudadanos y residentes.

Existen, sin embargo, importantes diferencias entre esos carnés de identidad y los nuevos permisos de conducir estadounidenses. La mayoría de los pasaportes electrónicos y DNI de proximidad (sin contacto) incorporan una etiqueta RFID que cumple el estándar industrial ISO 14443 (una norma desarrollada específicamente para tarjetas de identificación y pago, que incorpora cierto grado de seguridad y privacidad). Los nuevos carnés de conducir estadounidenses utilizan, en cambio, el estándar de RFID EPCglobal Gen 2, una técnica concebida para el seguimiento de productos en almacenes, donde lo que se busca no es la seguridad sino la máxima facilidad de lectura.

Mientras el estándar ISO 14443 incluye un rudimentario cifrado y requiere que las etiquetas se acerquen a un escáner para poderse leer (a una distancia de centímetros, más que de metros), las etiquetas Gen 2 no suelen estar cifradas y ofrecen una protección de datos mínima. Para leer los datos de un chip ISO14443 cifrado es preciso descifrar su código; sin embargo, para leer una etiqueta Gen 2 no se requiere ninguna habilidad es-

Así opera la RFID

En un sistema de RFID, un dispositivo lector interactúa a la vez con una etiqueta RFID y con una base de datos que contiene información asociada con dicha etiqueta. Las etiquetas se componen, como mínimo, de un circuito integrado codificado con un número identificador exclusivo y de una bobina metálica, o antena, que conduce la energía que recibe del lector.



EN LA TIENDA



Las cadenas de supermercados exploran usos de la RFID más allá del control de inventarios. El “espejo mágico” lee etiquetas RFID adheridas o engastadas en la ropa y presentan luego información sobre el producto, otros colores o artículos de complemento.

LILA RUBENSTEIN Y TOMMY MOORMAN (*ilustración*); CORTESIA DE AVERY DENNISON Y THEBIGSPACE (*espejo mágico*)

pecial, sólo un lector de ese código, fácil de conseguir y de uso común en almacenes de todo el mundo. Un pirata informático o un delincuente que posea tal dispositivo podría leer un carné de conducir con RFID a través de un bolso, una habitación o incluso desde el otro lado de un muro.

En abril de este año, más de 35.000 conductores del estado de Washington habían solicitado el nuevo permiso de conducir. Otros estados fronterizos (Arizona, Michigan y Vermont) han acordado su participación en el programa. El estado de Nueva York empezó a ofrecerlo en septiembre.

Pero el riesgo que entrañan esas tarjetas suscita cierta preocupación por nuestra seguridad. Aun cuando algún día se implantaran medidas de protección de datos más estrictas para bloquear accesos no autorizados a los datos de tarjetas RFID, numerosos defensores de la privacidad temen que los gobiernos utilicen los DNI de lectura remota para el control abusivo de sus ciudadanos.

El DNI chino incorpora datos que la mayoría de la gente consideraría una vergonzosa invasión del terreno personal: salud, historial reproductivo, situación de empleo, religión, grupo étnico e incluso el nombre y número de teléfono del casero del titular de la tarjeta. Más tenebroso todavía, esas tarjetas forman parte de un proyecto más amplio que cubrirá las ciudades chinas con un manto de técnicas avanzadas de vigilancia. Michael Lin, vicepresidente de Técnica de Seguridad Pública China (la compañía privada que suministra tarjetas RFID para este programa), no se arredró al describirlas para el *New York Times* como "un medio para el control futuro de la población". Y aunque otros gobiernos no aprovechen el potencial controlador de las nuevas tarjetas, hay pruebas evidentes de que las compañías ansiosas de información sí lo harán.

Una vida "etiquetada"

Si la idea de que las etiquetas de identificación por radiofrecuencia sirvan para espiar a individuos nos parece artificiosa, fijémonos en una patente de IBM registrada en 2001 y concedida en 2006. En ella se exponen con todo detalle las instrucciones de uso de las tarjetas para el seguimiento y análisis de conductas, aun cuando el acceso a bases de datos oficiales no exista o esté rigurosamente limitado. Bajo el título "Identificación y seguimiento de personas que utilicen artículos provistos de etiquetas RFID en entornos de almacén", describe con frialdad la capacidad de la RFID para la vigilancia en un mundo con lectores de RFID ("unidades de seguimiento personal") conectados en red para observar de cerca los movimientos de las personas, en casi cualquier lugar donde se congreguen: supermercados, aeropuertos, estaciones de tren y de autobuses, aviones, ascensores, trenes, aseos, polideportivos, bibliotecas, teatros y museos.

Un escáner estratégicamente situado puede leer las etiquetas RFID que porta una persona. Cuando un cliente circula por el supermercado, los escáneres repartidos por el establecimiento captan las señales de radio que emiten sus etiquetas RFID, con lo que se rastrea su movimiento. La unidad de seguimiento personal puede guardar registro de los anaqueles visitados por ese cliente, así como de las horas de las visitas.

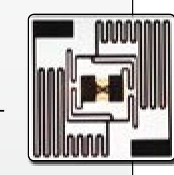
El hecho de que no se almacenen datos personales en la etiqueta no presenta ningún problema, aclara IBM, puesto que la información personal se obtiene cuando la persona utiliza su tarjeta de crédito, tarjeta bancaria, de compra o similar. Con una sola operación que vincule el número RFID de la etiqueta y la identidad de portador, la tarjeta se convierte en delegada de su poseedor. IBM había imaginado que el seguimiento de las personas se llevaría a cabo mediante etiquetas miniatura fijadas en artículos de consumo, pero parece que la generalización de las etiquetas de RFID va a llegar con los carnés de conducir de última generación. Los nuevos permisos de conducir del estado

La autora

Katherine Albrecht es doctora en educación por la Universidad de Harvard. Dirige CASPIAN, una organización de 15.000 miembros que trabaja para la defensa de la privacidad del consumidor; se oponen a los sistemas de vigilancia en tiendas. Albrecht es coautora de dos libros sobre las amenazas a la privacidad y seguridad individual que comporta el uso de la RFID por empresas y gobiernos.

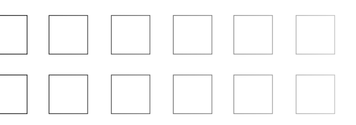
Tipos de etiquetas

Los estándares técnicos de EPCglobal permiten agrupar las etiquetas RFID con arreglo a sus capacidades mínimas. Cada clase añade nuevas propiedades a las de la clase básica 1, que es "pasiva" (depende de que un lector inicie la comunicación y le suministre energía). Las etiquetas pasivas se leen a distancias de hasta 9 metros; las activas hasta 90 o más.



	Funciones mínimas	Aplicaciones
CLASE I (Pasiva)	• Número identificador exclusivo • Función para desactivar la etiqueta • Memoria programable una sola vez • Las nuevas versiones de "Gen 2" pueden reprogramarse y protegerse mediante contraseña	• Piezas e inventarios • Permiso de conducir mejorado (EE.UU.) • Tarjeta de acceso
CLASE II (Pasiva)	• Número ID ampliado • Memoria adicional, reprogramable • Acceso por contraseña	• Pasaporte electrónico • Tarjeta de crédito • DNI
CLASE III (Semi-pasiva)	• Uno o varios sensores y una fuente de alimentación	• Sensores en contenedores y almacenes
CLASE IV (Activa)	• Transmisor y fuente de alimentación • Inicia comunicación con lector u otra etiqueta	• Llavero con mando • Etiqueta de animal • Pase de peaje

EPCGLOBAL, INC. (*logo*); VERICHIP CORPORATION (*chip con moneda*); ALIEN TECHNOLOGY CORPORATION (*etiqueta RFID*)



de Washington serían una solución ideal para el seguimiento de la clientela en una tienda, pues ya son legibles por los escáneres de inventario Gen 2 que utilizan hoy en EE.UU. los supermercados de Wal-Mart, Dillard's y American Apparel.

La utilidad comercial de los sistemas de seguimiento aumentará conforme empecemos a llevar encima, incluso en la ropa, artículos con etiqueta RFID. Hoy día circulan decenas de millones de tarjetas bancarias de lectura remota provistas de etiquetas RFID, además de millones de placas de acceso de empleados. También llegan a las ciudades estadounidenses los abonos de transporte público basados en RFID, muy extendidos en Europa y Japón. La unidad de seguimiento personal de IBM no es más que una patente, por ahora, pero el parque de atracciones inglés Alton Towers ofrece un ejemplo real de la capacidad de seguimiento de la identificación por radiofrecuencia. Cuando un visitante entra en el parque, se le ofrece una muñequera con RFID en la que va codificado un número de identificación exclusivo. Una red de lectores RFID ubicados en puntos estratégicos detecta cada muñequera que se pone a su alcance y activa las videocámaras cercanas. La grabación obtenida de cada visitante se almacena en un archivo etiquetado con su ID, que se le entrega al final de la jornada en un DVD de recuerdo.

Protección del público

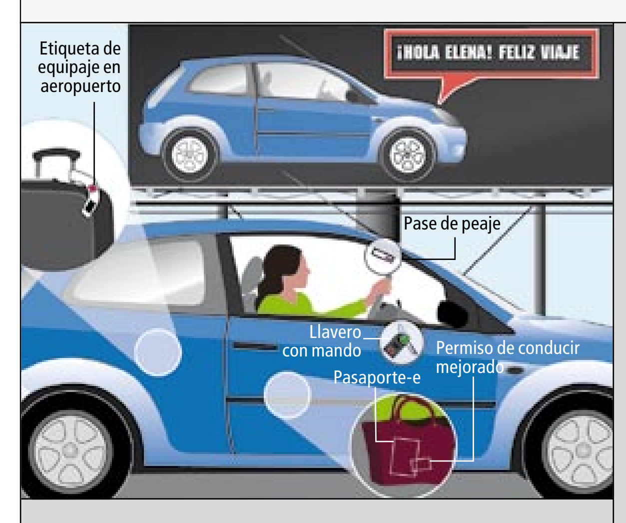
Si las etiquetas RFID permiten que un parque de atracciones grabe vídeos detallados y personalizados de miles de visitantes al día, imagínese lo que podría hacer un gobierno, y no digamos los comerciantes o delincuentes. Por eso, en defensa de la privacidad del consumidor, nos oponemos rotundamente al uso de la RFID en DNI o artículos de consumo individual. Ya desde 2003, nuestra organización CASPIAN (Consumidores Contra la Numeración y la Invasión de la Privacidad en Supermercados, en inglés), junto con la Cámara de Compensación de Derechos de Privacidad, el Centro de Información sobre Privacidad Electrónica, la Fundación Frontera Electrónica, la Unión de Libertades Civiles Americanas y otras 40 organizaciones en pro de la privacidad y las libertades civiles, reconoció esta amenaza y publicó un documento en el que tachaba de improcedente el seguimiento de personas mediante la identificación por radiofrecuencia.

En respuesta a esos temores, en docenas de estados se han promulgado decretos que protegen al consumidor de la RFID, pero todos ellos han sido anulados o invalidados por la fuerte oposición que ejerce la industria del sector. Cuando el senado de New Hampshire votó en 2006 a favor de un decreto que habría impuesto a la RFID una reglamentación estricta, una enmienda de última hora lo sustituyó por un estudio de dos años. Aquel mismo año, en California, un decreto que habría prohibido el uso de RFID en documentos oficiales fue aprobado por ambas cámaras de la legislatura, pero se estrelló contra el veto del Gobernador Arnold Schwarzenegger.

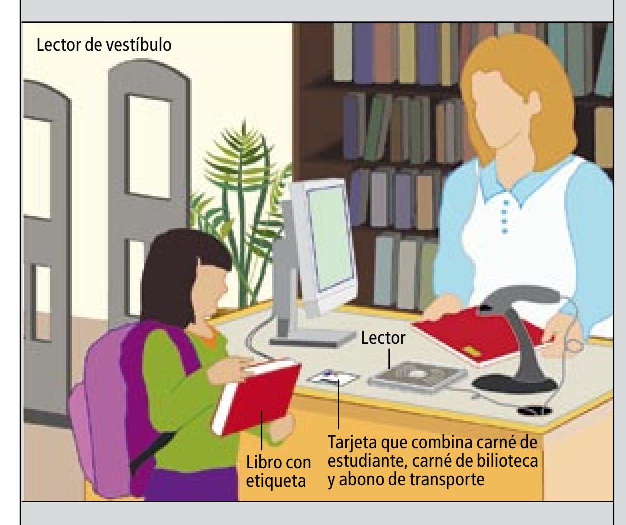
A escala federal, no se ha aprobado ningún decreto de gran alcance que proteja al consumidor. Por el contrario, el grupo de trabajo (*task force*) de técnica avanzada de los republicanos

RFID en nuestro día a día

Aumenta el número de artículos de uso cotidiano con etiquetas RFID. De ello se benefician los consumidores y las empresas, en



En un viaje pueden intervenir múltiples etiquetas RFID: pases de peaje y llaveros con mando a distancia, pasaportes electrónicos, permisos de conducción y etiquetas para equipaje en aeropuertos.



Las escuelas y bibliotecas públicas incorporan etiquetas en los libros, carnés de biblioteca y carnés de estudiante. En el distrito de Columbia, una nueva tarjeta con etiqueta RFID operará a modo de "tarjeta única": carné de estudiante, carné de biblioteca y abono de transporte público, todo en una.

DIRECTRICES VOLUNTARIAS

EPCglobal, Inc., organización que fija normas para las etiquetas RFID, establece también directrices para utilizarlas a modo de "códigos electrónicos de producto" (CEP) en bienes de consumo.

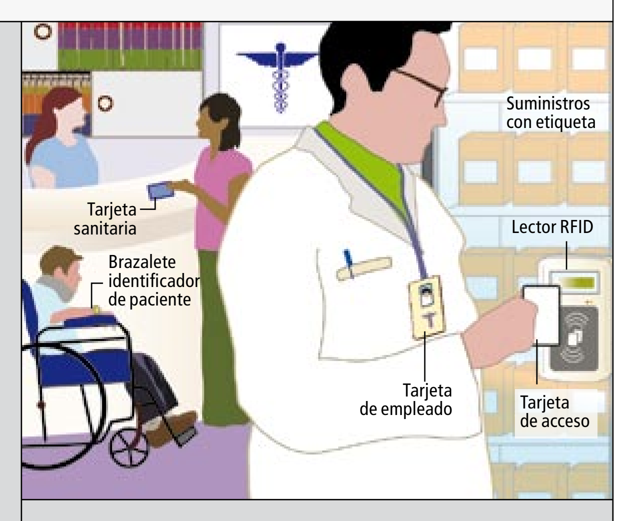
Advertencia: Se advertirá claramente a los consumidores de la presencia de CEP en el producto o el envoltorio mediante el uso de un logotipo o identificador de CEP.

Elección: Se informará a los consumidores de la opción de quitar o desactivar las etiquetas CEP de los productos que adquieren.

Educación: Las compañías que utilicen etiquetas CEP familiarizarán a los consumidores con el logotipo CEP y les facilitarán la comprensión de la técnica.

Registros: Los datos de consumidores asociados a las etiquetas serán recogidos, almacenados y protegidos por las compañías miembros de EPCglobal en cumplimiento de las leyes aplicables.

el control de la seguridad y la administración de inventarios. Facilitan también los estudios de mercadotecnia.



Las empresas suelen distribuir tarjetas de acceso y de empleado con etiqueta identificativa. El uso de etiquetas en hospitales ayuda a controlar el acceso a suministros médicos y a realizar el seguimiento de los pacientes.



Se insertan etiquetas en las mercancías de consumo para el control de inventarios; en algunos almacenes se entregan a los compradores lectores de etiqueta para visualizar información o descuentos. Los supermercados deberían ofrecer al cliente la posibilidad de desactivar las etiquetas en los artículos comprados, pero muchos no lo hacen.

LILA RUBENSTEIN

en el Senado ha ensalzado las aplicaciones de la identificación por radiofrecuencia, pues las considera "estimulantes técnicas novedosas" que encierran "inmensas promesas para nuestra economía"; se ha comprometido a proteger la RFID contra reglamentos y leyes.

En la Unión Europea por lo menos se examina la situación. La Comisión Europea, brazo ejecutivo de la UE, reconoce que la RFID puede plantear graves problemas de privacidad. Para ello abrió en julio de 2006 un período de consulta pública. Con todo, hay pocas esperanzas de que se establezcan disposiciones reguladoras. En marzo de 2007, Viviane Reding, comisaria europea de Sociedad de la Información y Medios de Comunicación, anunciaba que la Comisión no iba a regular la RFID, sino que dejaría a las propias empresas que se autorregulasen. En su opinión, deben aligerarse, no sobrecargar, las leyes para que este sector pueda cobrar impulso.

Para nuestro infortunio, la autorregulación de la industria es demasiado débil para proteger a la población de los riesgos de la identificación por radiofrecuencia. EPCglobal, el organismo industrial que establece estándares técnicos para las etiquetas de RFID, elaboró asimismo una serie de directrices para el uso de estos chips en supermercados. Entre otras medidas, recomiendan que se avise a los consumidores siempre que adquieran productos etiquetados (con un logotipo RFID reconocible, por ejemplo). Sin embargo, cuando Checkpoint Systems, afiliada a EPCglobal, diseñó etiquetas RFID para ocultar en la suela de los zapatos —en clara infracción de las propias normas de este organismo—, Mike Meranda, entonces presidente de EPCglobal, adujo que, al ser las directrices de aplicación voluntaria, nada podía hacer al respecto su organización.

El Departamento de Licencias del estado de Washington intenta convencer a los ciudadanos de que sus datos personales están a salvo, dado que la etiqueta RFID de los nuevos permisos de conducir carecen de fuente de alimentación y no contienen ninguna información de identificación personal —aunque ello nada tiene que ver con el posible uso de la tarjeta para seguimiento—. La falsa sensación de seguridad que transmiten esas declaraciones oficiales podría en ciertos casos resultar perjudicial. La Red Nacional para el Fin de la Violencia de Género, que de palabra se opone al uso de RFID en DNI y artículos de consumo, ha presentado una moción legislativa que describe el modo en que los maltratadores podrían utilizar esta técnica para acechar y vigilar a sus víctimas.

Entre tanto, el tren de la RFID avanza sin tregua. En el estado de Washington se han concedido ya 10.000 carnés con RFID. Las posibilidades de abuso son grandes, y no dejarán de crecer. En fecha reciente, ese estado ha realizado un tímido esfuerzo normativo: ha aprobado una ley por la cual la lectura no autorizada de una etiqueta con intención de fraude, sustracción de identidad o cualquier otro fin ilegal se considera un delito de clase C, sujeto a cinco años de prisión y multa de 10.000 dólares. Pero esa ley nada dice de la prohibición de escanear con otros fines, como los relacionados con la mercadotecnia o el control de la población. Riesgos que despreciamos bajo nuestra responsabilidad.

Bibliografía complementaria

SPYCHIPS: HOW MAJOR CORPORATIONS AND GOVERNMENT PLAN TO TRACK YOUR EVERY MOVE WITH RFID. Katherine Albrecht y Liz McIntyre. Thomas Nelson, 2005.

RADIO-FREQUENCY IDENTIFICATION (RFID): ADDRESSING CONCERNS OVER INFORMATION COLLECTION AND USAGE. Vídeo sobre una mesa redonda en la Escuela Legal de la Universidad de Washington, 19 de julio de 2007. Disponible en www.law.washington.edu/lct/Events/rfid

PRIVACY IMPACT ASSESSMENT FOR THE USE OF RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY FOR BORDER CROSSINGS. Departamento de Seguridad Nacional de EE.UU., 22 de enero de 2008.

IDENTIDAD EN LA RED

En un entorno de múltiples identidades, computación distribuida y redes sociales, aparecen nuevas amenazas a la privacidad. Se requieren nuevas soluciones al conflicto entre los derechos a la libertad informática, la identidad digital y la protección de datos

Ignacio Alamillo Domingo

CONCEPTOS BASICOS

- La identidad electrónica constituye un elemento clave en el ciberespacio. Nos permite interactuar, ser reconocidos y ejercer nuestros derechos en la red.
- El uso inapropiado de la identidad, un exceso de identificación y la interconexión masiva de aplicaciones y sistemas, sobre todo en la Red Semántica, suponen una amenaza a la privacidad.
- El futuro exige repensar las leyes de protección de datos, fomentar los sistemas federados de identidad con preferencias personales de los usuarios identificados y ampliar el derecho al anonimato en las transacciones. En suma, devolver al ciudadano el control de sus datos.

Un día laborable cualquiera, Laura sube al tren que le lleva al trabajo. Como cada mañana, aprovecha el trayecto para consultar, desde su agenda electrónica, las novedades de prensa del día; para ello debe identificarse como cliente de la compañía telefónica y de la editorial que publica las noticias en línea. Al llegar a la empresa, emplea su tarjeta corporativa para acceder al edificio y a la red interna de la organización; se identifica ante las aplicaciones de negocio, de Internet y de correo electrónico, mientras accede con su identidad a la cuenta de música en línea en Internet.

Durante la pausa del desayuno, se identifica ante LinkedIn y Facebook para actualizar su perfil de usuario y compartir informaciones personales con los demás miembros de la red social. Antes de acabar la jornada, aprovecha para entrar, mediante su identidad financiera, en el servicio de banca electrónica y realizar algunos pagos pendientes. Ya en casa, después de cenar, emplea su certificado digital para presentar la declaración de la renta, antes de que se cierre el plazo. A lo largo del día, Laura ha utilizado múltiples identidades electrónicas, cada una para un propósito distinto.

La identidad electrónica corresponde, en esencia, a un conjunto de datos, o atributos, que nos diferencian del resto de las personas: nuestro nombre y apellidos, el nombre del padre y de la madre, el DNI, etcétera. También las máquinas cuentan con datos que las identifican: la dirección IP o el nombre de dominio en Internet, entre otros. Se consideran identidades "electrónicas" porque se asignan, almacenan y gestionan por medios electrónicos, en bases de datos de identidad. Según la función que desempeñan, las identidades se distinguen entre personales, corporativas y de cliente.

La "identidad electrónica personal" nos identifica de forma autónoma, sin conexión con organización ninguna. Se trata de una identidad regulada por el Estado y válida dentro de su territorio. Se basa en procesos robustos de identificación física. En España se ha venido acreditando mediante la partida de nacimiento, el DNI y la Tarjeta de Residencia.

1. MULTIPLES IDENTIDADES electrónicas configuran nuestra personalidad en la Red. En función de nuestro "interlocutor" y del propósito de la comunicación ("chatear" con un amigo, pujar en una subasta de Ebay, participar en un foro de cocina, realizar un pago mediante tarjeta de crédito, etcétera) mostramos una u otra de nuestras múltiples identidades parciales.


Bienvenido de
Identifícate
acceder a tu cuenta.
Seudónimo
He olvidad
dónimo
Contraseña
He olvidado
$ $
VISA
utilizando un
¿Ti
nes dificultades para identificarte? Obtener
Protege tu cuenta:
web que
aparece en el navega

Identidades electrónicas

La identidad electrónica corresponde a un conjunto de datos (atributos) que nos diferencian del resto de las personas o entidades en un ámbito concreto. Según la función de la identidad y nuestra relación con el emisor de la misma, las identidades electrónicas se clasifican en:

Según la función...

PERSONAL

Nos identifica de forma autónoma, sin conexión con ninguna organización. Está regulada por el estado y es válida dentro de su territorio. Se basa en procesos robustos de identificación física (ejemplos: partida de nacimiento, DNI, tarjeta de residencia).

CORPORATIVA

Nos vincula con una organización pública o privada mediante una relación jurídica de pertenencia o vinculación. Suele construirse sobre el documento de acreditación de la identidad física personal (ejemplos: tarjeta de trabajador o de funcionario, de profesional colegiado).

DE CLIENTE

Nos vincula con una organización pública o privada con la que se establece una relación de negocio (ejemplos: tarjeta de claves de identificación bancaria, tarjeta cliente del supermercado).

Según el emisor...

DE TERCERA PARTE

Nos la suministra una organización o persona ajena a nosotros. Sirve para relacionarnos con organizaciones y personas ajenas al emisor (ejemplo: firma electrónica certificada).

DE SEGUNDA PARTE

Nos la suministra una organización o persona ajena a nosotros. Sirve sólo para relacionarnos con el emisor.

DE PRIMERA PARTE

La emitimos nosotros mismos. Promete un nuevo modelo de privacidad bajo el control del usuario (ejemplos: identidades creadas en Second Life, Facebook, LinkedIn).



Se trata de una "identidad nuclear" o "identidad base", ya que sobre la misma se construyen los tipos de identidad restantes y se cruzan bases de datos de identidad.

La "identidad electrónica corporativa" refleja una relación jurídica de pertenencia o vinculación con una organización pública o privada. Con frecuencia se construye sobre el documento que acredita la identidad física personal (tarjeta de trabajador, de funcionario, de profesional colegiado, etcétera).

La "identidad electrónica de cliente" nos vincula con una organización pública o privada con la que establecemos una relación comercial. Esta identificación es obligatoria en algunos casos (claves para realizar gestiones bancarias por Internet, tarjeta de abonado para acceder al club deportivo) y voluntaria en otros (tarjeta cliente del supermercado).

La frontera entre estos tipos de identidad no resulta siempre evidente. Algunas de las identidades que han nacido de una relación entre empresa y cliente han adquirido tanta relevancia, que la ley ha otorgado al cliente el derecho de mantenerlas incluso cuando termina la relación comercial, convirtiéndolas en identidades personales. El ejemplo más paradigmático de ese tipo de identidad corresponde al número de teléfono móvil, pues puede "portarse" de un proveedor de servicios de telefonía a otro y conservarse conforme a la regulación.

Todas estas identidades electrónicas corresponden a identidades "de segunda o tercera parte", porque nos son suministradas por organizaciones o personas ajenas a nosotros. Las de "segunda parte" sirven sólo para relacionarnos con la entidad o persona suministradora, mientras que las de "tercera parte" sirven para relacionarnos con organizaciones y personas distintas del suministrador (por ejemplo, la firma electrónica certificada).

Más recientemente, con el advenimiento de la Web 2.0, los propios usuarios hemos empezado a actuar como emisores o garantes de nuestra propia identidad, mediante la divulgación de datos personales que permiten que terceras personas nos reconozcan. Hallamos ejemplos de ello en los avatares de los mundos virtuales (Second Life) y en las fichas personales de sistemas de gestión de comunidades y redes sociales (Facebook,



SECONLIFE, FACEBOOK Y LINKED IN (*logos*)

LinkedIn). Son las identidades "de primera parte", que prometen un nuevo modelo de privacidad bajo el control del usuario. De hecho, se habla ya de un nuevo paradigma en la gestión de la identidad, basado en la gestión por el propio usuario de todo el ciclo de vida de su identidad, con mayor control sobre la divulgación de sus datos personales.

Propiedades

Según un trabajo reciente de la Organización para la Cooperación y el Desarrollo Económico (OCDE), la identidad electrónica presenta una serie de propiedades: es social, subjetiva, valiosa, referencial, compuesta, consecuencial, dinámica, contextual y potencialmente equívoca.

La identidad electrónica se considera un atributo social porque que se refiere a personas que viven en sociedad y que, por tanto, necesitan poder reconocer con quién interactúan. Es también subjetiva, pues depende de las percepciones que nosotros mismos u otros nos atribuyen. Es valiosa, porque la acumulación de datos históricos relativos a nuestros actos resulta en un capital informacional, que puede emplearse para establecer relaciones personalizadas y para tomar decisiones relativas a nuestras relaciones interpersonales con un mayor grado de confianza (así lo ha demostrado la teoría de juegos).

La identidad electrónica es referencial porque no constituye una persona, sino una referencia a la misma. Incluso en el caso de que una persona configure diversos perfiles propios, o si terceros desarrollan perfiles sobre ésta, en último término el conjunto de atributos que la identifican deben referirse a ella de forma fiable.

La identidad electrónica constituye, asimismo, un atributo compuesto. Mientras que algunas informaciones son suministradas por nosotros mismos (las de "primera parte"), otras son construidas por terceros, sin nuestra participación. Dado que la información de identidad habla de nuestras acciones pasadas, la divulgación, o no, de la misma puede generar daños; se considera por ello un atributo consecuencial.

La identidad electrónica es dinámica porque sufre constantemente cambios y modificaciones; cualquier fichero con datos de identidad puede quedar obsoleto en un momento determinado. Es también contextual, ya que en función del contexto utilizaremos una u otra de nuestras múltiples identidades parciales. Por fin, la identidad electrónica es potencialmente equívoca, puesto que el proceso de identificación y asociación de datos de identidad se halla intrínsecamente expuesto a errores.

Todos tenemos numerosas identidades (parciales), adecuadas a los distintos roles y actividades que realizamos, cuyo uso está defendido por las leyes de protección de datos personales. Algunas de dichas identidades se consideran un bien público y resultan de uso obligatorio (DNI). Otras se consideran de propiedad privada y su uso es voluntario (certificado de firma emitido por un prestador privado) o se encuentra asociado a una relación jurídica concreta (contraseña suministrada por una entidad financiera). La identidad electrónica de segunda y tercera parte se encuentran, por tanto, privatizadas, mientras que la de primera parte es de nuestra titularidad.

Mecanismos de autenticación

En ocasiones, la identidad electrónica permite la autenticación: es decir, la posibilidad de asociar a una de nuestras identidades mecanismos que nos permitan demostrar quiénes somos y operar en la Red.

Entre los mecanismos de autenticación más empleados destacan las contraseñas, las contraseñas dinámicas, las de un solo uso y las basadas en *hardware* portátil ("tokens USB");

El autor

Ignacio Alamillo Domingo es abogado y consultor sénior de seguridad de la información en la Secretaría de Telecomunicaciones y Sociedad de la Información de la Generalidad de Cataluña.

Cómo proteger nuestra privacidad



Vivimos en un mundo interconectado en el que se nos asignan y gestionamos múltiples identidades. Nuestras operaciones, transacciones y relaciones digitales generan rastros, documentos y registros que, recolectados y almacenados por terceros, y usados de forma indebida, podrían resultar en intromisiones a nuestra privacidad. Sólo nosotros deberíamos determinar quién puede acceder a nuestros datos y con qué propósito.

Disponer de varias identidades apuntala nuestro derecho fundamental a la protección de datos. Permite limitar el acceso a nuestra información personal y evita el cruce de ciertas operaciones (el cruce de datos no puede realizarse sin nuestra autorización). Veamos algunos ejemplos:

IDENTIDAD CORPORATIVA
Nuestra identidad corporativa está sujeta a controles por parte de la empresa para la que trabajamos, que sólo debe cederla en ciertos casos permitidos por la ley.



MULTIPLES IDENTIDADES DE CLIENTE
Al tener varias identidades de cliente, la empresa para la que trabajamos, o terceros no autorizados, difícilmente podrá averiguar qué prensa electrónica leemos durante los descansos en la oficina.



IDENTIDADES ANONIMAS
Las identidades parcialmente anónimas, o basadas en pseudónimos, en redes sociales nos permiten realizar transacciones de forma completamente anónima (el anonimato puede desvelarse sólo mediante mandamiento judicial).

los certificados digitales X.509 de identidad, emitidos por varios prestadores (verbigracia, Agencia Catalana de Certificación) a empleados públicos (T-CAT) y a ciudadanos (idCAT), sobre todo en entornos de movilidad y de tramitación a distancia; las identificaciones electrónicas nacionales (DNI electrónico); y los tiques de autenticación remota o delegada (SAML, Kerberos).

Dado que los mecanismos de autenticación son múltiples y las identidades que se nos asignan tienen distintas cualidades y limitaciones de uso, hablamos de sistemas multinivel de identidad y autenticación, que se clasifican en grados de seguridad según un análisis de riesgos.

Las entidades financieras emplean sistemas de contraseña para la identificación de sus clientes en la banca electrónica, combinados con tarjetas de coordenadas (incluyen entre 20 y 50 contraseñas que se solicitan de forma aleatoria, para “firmar” las operaciones). Las administraciones públicas emplean certificados electrónicos reconocidos de firma electrónica, para la identificación de los ciudadanos.

¿Identidades únicas o federadas?

Se debate en los círculos de expertos el concepto de “identidad única”. En virtud de esta propuesta emplearíamos una sola ficha de identidad, con un único proveedor, para identificarnos frente a todas las organizaciones y terceras personas.

Sin embargo, en el sector privado así como en la mayoría de administraciones públicas, dicha solución topa con ciertas dificultades en cuanto a la conveniencia o capacidad legal de crear y asignar códigos de identificación universal. En numerosos Estados la sensibilidad por la protección de los datos personales impide el establecimiento de esa clase de modelos. En Austria, por ejemplo, pese a asignarse un código único de identidad a todos los nacionales y residentes, la ley prohíbe el empleo directo del mismo. Cuando se precisa identificar a una persona, su Tarjeta de Identidad genera un código sectorial específi-

co para ese uso, para evitar que se produzca el cruce de datos del ciudadano a través de sectores distintos.

Por tanto, debido a la presión legal de la privacidad, en la Red vamos a disponer de diversas y variadas identidades, con sus correspondientes mecanismos de autenticación. Para resolver esta situación se ha propuesto la "federación de identidades": un entorno tecnológico, organizativo y jurídico basado en normas de confianza mutua, que permite compartir la identidad y la autenticación de los usuarios entre varios sistemas.

Las soluciones de gestión y federación de identidades, muchas de ellas basadas en el estándar SAML ("Security Assertion Markup Language"), promovido por OASIS y publicado por ISO, permiten que varios proveedores de identidad y de servicios puedan colaborar para llevar a cabo operaciones referidas a una persona, con control por parte de ésta del uso que se hace de su identidad y de los mecanismos de autenticación empleados.

La federación de identidades facilita también el control, por parte del afectado, del intercambio de datos personales. Ello permite el desarrollo de aplicaciones informáticas y comunidades alrededor del usuario, donde él es el actor y protagonista, y puede ejercer las facultades del derecho a la protección de datos personales.

Identidad y firma electrónica

Si bien el concepto de firma electrónica es más amplio que el de identidad electrónica, ambos guardan una estrecha relación técnica y legal. El primer uso de la firma electrónica se produce precisamente en el ámbito de la seguridad informática, a modo de mecanismo de autenticación de identidad.

En un segundo escenario, la firma electrónica se considera un elemento esencial de los documentos electrónicos. En esta concepción, más madura, el valor de la firma electrónica deriva de la necesidad de que los documentos sean auténticos, atribuibles a las personas, "firmados" en el sentido cultural, jurídico, administrativo e histórico del término. Se produce así el reconocimiento legal de la firma electrónica avanzada, desgajada de la simple comprobación de la identidad personal.

La equiparación legal entre la firma electrónica y la firma escrita no resulta trivial. Supone la equivalencia entre la persona y su agente electrónico, que es quien materialmente firma por él. Un documento carece, por tanto, de valor si no está firmado, aunque haya sido producido y conservado de forma segura.

Un tercer paradigma, al que ya estamos asistiendo, considera la identidad y la firma electrónica como un elemento de capacitación de las personas en el ámbito electrónico. De esta forma, se enriquece el concepto para ir más allá de la identidad personal. La identidad y la firma electrónica incorporan otros atributos de la persona: capacidad de actuación (asociada a la edad o la nacionalidad), capacidad profesional (acreditada por la corporación correspondiente), laboral y capacidad de representación de otros (apoderamientos).

El usuario dispone de más de una firma electrónica; para cada uso deberá elegir la más apropiada. Esta explosión de certificados digitales para las relaciones electrónicas supone la proliferación de prestadores de servicios de certificación, públicos y privados. Hemos inaugurado la era de las entidades de validación.

En la actualidad, gran parte de la población está capacitada para relacionarse electrónicamente con entidades públicas y privadas. Ello ha resultado en la aparición de un cuarto paradigma. Este escenario abre la posibilidad de que el usuario ya no necesite aportar cada vez los documentos acreditativos (de personalidad, capacidad o representación) ante cada organismo; asimismo, facilita la integración de los procedimientos de negocio.

En este estadio, la identidad y la firma electrónica se consideran un ancla entre dos mundos (el físico y el electrónico), de forma que el agente informático que representa al ciudadano adquiere las mismas capacidades frente a la administración o la empresa. Ello fomenta la incorporación de la firma electrónica a los documentos de legitimación, como la tarjeta sanitaria (en algunos Estados y Comunidades Autónomas incorpora ya un microchip con identidad y firma electrónica) o las licencias profesionales o de conducción.

El paradigma más avanzado

El quinto y más avanzado paradigma considera la identidad y la firma electrónica elementos imprescindibles de garantía de los derechos y libertades personales, en una sociedad con un número creciente de conexiones y accesos a la información personalmente identificable.

La protección de datos limita los sistemas de identidad y de capacidad electrónica. Nos defiende de las potenciales consecuencias negativas de la identificación masiva de personas y de la disposición de redes públicas que permiten el acceso a todas las bases de datos (públicas y privadas) con informaciones de estas personas. Por ese motivo, los sistemas de identidad y capacidad electrónica deben permitir la participación de las personas identificadas y, lo que reviste mayor importancia,

LAS 7 LEYES DE LA IDENTIDAD

Para conciliar la gestión de la identidad en la Red con la protección de datos personales, se ha propuesto una estrategia que se resume en los siguientes principios:

1 Exigir el **control** y **consentimiento** del usuario.

2 **Minimizar** la cantidad de **información** divulgada y **restringir** el **uso** posterior.

3 Divulgar **sólo** a **terceros** justificados y **fiables**.

4 Usar identificadores omnidireccionales para el uso en entidades públicas y unidireccionales para entidades privadas (**identidad direccional**).

5 Respaldar la **pluralidad** de **técnicas** de identidad y operadores.

6 Integrar al usuario en el sistema distribuido mediante mecanismos de **comunicación hombre-máquina**.

7 Garantizar al usuario una **experiencia** simple y **coherente** en todos los contextos.

LUCY READING-IKKANDA



2. EN LA RED SEMANTICA, las máquinas "hablan" entre ellas acerca de nosotros, intercambiando datos sobre nuestra persona, a veces sin nuestro consentimiento.

el control por parte de éstas del acceso a la información y la autorización para el intercambio en línea de sus datos.

Identidad en la Web 2.0

Para conciliar los sistemas de gestión de identidad y capacidades con la protección de datos personales se han propuesto las "siete leyes de la identidad". Esta iniciativa, adoptada ya por algunas instituciones canadienses, establece siete principios: control y consentimiento del usuario, divulgación mínima para uso restringido, justificación de terceros, identidad direccional, pluralismo de técnicas y operadores, integración usuario-máquina y experiencia coherente en todos los contextos.

Hallamos un ejemplo de aplicación de esos siete principios en el sistema de selectores de identidad del CardSpace de Microsoft (antes InfoCard). En este sistema, de acuerdo con el principio de control y consentimiento del usuario, sólo el usuario puede seleccionar y enviar un conjunto de alegaciones de identidad a los destinatarios.

El usuario puede crear tarjetas de información propias, sin necesidad de proveedores externos de identidad (aunque en ese caso la información tendrá un valor distinto para el destinatario, que no siempre confiará en las alegaciones hechas por el usuario).

De acuerdo con el principio de pluralidad de técnicas y operadores, el usuario podrá construir múltiples identidades digitales, distintas en cuanto a la cantidad y a la calidad de la información. Contará con varias tarjetas de información en su cartera virtual y seleccionará la más apropiada para cada destinatario.

Algunas tarjetas no contendrán ningún dato nominativo, sino atributos como el sexo o la edad; otras contendrán datos nominativos que les permitirán realizar, por ejemplo, transacciones electrónicas con las administraciones públicas o con organizaciones privadas. Se cumplen así las leyes de divulgación mínima y de justificación de terceros.

La capacidad del usuario de crear y emplear múltiples tarjetas unidireccionales (que le permiten relacionarse cada una con un destinatario concreto) le protege de la divulgación innecesaria de correlaciones de identidad, que puedan ser compartidas entre sitios de Red para configurar perfiles de preferencias; ello cumple el principio de "identidad direccional" (por analogía con el mundo físico, se considera que la identidad posee, además de magnitud, dirección).

El modelo de selectores de identidad CardSpace permite, por tanto, resolver el conflicto entre la gestión de la identidad en la Web 2.0 y la protección de datos personales, haciendo que el usuario sea quien decide la cantidad, finalidad y límites de uso de la información de identidad que comparte.

Identidad en la Red Semántica

El otro dominio novedoso en el que trabajan los expertos es el de la identidad en la Red Semántica. El reto principal consiste en lograr que las máquinas "hablen" entre ellas acerca de personas (identidades parciales) concretas.

La Red Semántica constituye una iniciativa del W3C ("World Wide Web Consortium"), el consorcio que define los principales estándares de Internet. La Red se concibe como un sistema informático distribuido, capaz de realizar funciones y tareas sociales, con las necesarias interfaces de interacción con las personas físicas [*véase* "La Red Semántica en acción", por Lee Feigenbaum, Ivan Herman y otros, *Investigación y Ciencia*, febrero de 2008].

Dichas interfaces se consideran "saltos" fuera de la Red Semántica, actuaciones humanas residuales en un mundo cada vez más automatizado. Es decir, se busca la intervención de la persona sólo cuando la máquina no es capaz de completar el proceso sin dicha actuación personal; esa intervención humana suele requerir de una firma electrónica.

En ese sentido, la Red Semántica persigue que las máquinas adquieran una comprensión de la información que circula por la Red, de forma que se les pueda delegar la realización de tareas que requieren entendimiento e inteligencia. El modelo habitual de relación se basará, por tanto, en diálogos máquina-

© *iStockphoto*/VASILIY YAKOBCHUK

máquina acerca de nosotros, las personas y nuestras identidades, lo que requiere estándares de identidad, seguridad y confianza.

Una de las propuestas más elaboradas viene dada por el estándar abierto SAML. Se encuentra en el núcleo de los sistemas de gestión y federación de identidad más importantes; ofrece una serie de mecanismos que permiten aplicar la protección de datos personales en un entorno de Red Semántica.

SAML permite el establecimiento de pseudónimos entre un proveedor de identidad y un proveedor de servicios, de forma que no en todos los casos sea necesario liberar toda la información de identidad de la persona con la que se desarrolla un negocio. Esos pseudónimos evitan la formación de correlaciones inapropiadas entre dos proveedores de servicios distintos, inevitable si se utilizase un identificador único o global, como el DNI electrónico.

SAML opera mediante identificadores transitorios o de un solo uso. Cada vez que el usuario accede a un proveedor de servicio, a través de una operación de autenticación por intermediación de un proveedor de identidad, lo hace con una nueva identidad, de forma que el proveedor de servicio no podrá reconocerlo.

Merced a los mecanismos de contexto de SAML, el usuario es autenticado al nivel de seguridad apropiado, ni insuficiente ni excesivo, para el recurso al que accede. Asimismo, SAML permite expresar entre proveedores el hecho de que un usuario haya consentido determinadas operaciones; por ejemplo, la federación de identidades entre dos proveedores.

Liberty Alliance, una asociación global que promueve normas y estándares de federación de identidad, que emplea y amplía el estándar OASIS, ha diseñado los sistemas pensando en la protección de datos personales, pieza fundamental de la confianza de los usuarios. Según la visión de Liberty, la información personal debe ser compartida bajo el consentimiento del usuario y de acuerdo con sus instrucciones. Ello implica que los proveedores deberán informar al usuario y obtener su consentimiento expreso.

Las especificaciones de Liberty permiten el almacenamiento de este acto de información al usuario y de su consentimiento. Ello se lleva a cabo mediante la especificación de cinco configuraciones de protección de datos personales que indican las preferencias de los usuarios respecto al uso de sus datos personales, descritas en lenguaje natural y en lenguaje P3P (de "Plataforma de Preferencias de Privacidad"). El usuario puede optar entre una privacidad estricta, privacidad con cautela, privacidad moderada, privacidad flexible y privacidad informal.

Conclusiones

La gestión de la identidad electrónica constituye uno de los principales retos de las redes telemáticas y uno de los elementos clave para la interoperabilidad. Arrastra tras de sí los desafíos de la autenticación, la firma electrónica y las capacidades de actuación.

El nuevo contexto de actuación se encuentra marcado por la heterogeneidad y la complejidad. Por un lado, operan numerosas identidades (públicas, privadas, nacionales, regionales, locales, sanitarias, financieras, etcétera). Por otro, existe una tendencia a la reducción y generalización de las identidades y al incremento de las identidades de "primera parte" (sobre todo en las redes sociales).

Asimismo, crece el número de proveedores en red de atribuciones y capacidades (administraciones públicas, registros jurídicos y notariales). Aumenta el número de entidades privadas que tienden a la especialización y al consumo en línea mediante servicios en red automatizados.

La ley de protección de datos personales determina cuáles son las prácticas aceptables y limita los intercambios de información de identidad. Esas reglas deberán ampliarse para otorgar nuevas facultades de control a los usuarios, con el incremento consiguiente de las identidades basadas en pseudónimos y de las operaciones tornadas anónimas, esto es, aquellas en las que se han "borrado" las huellas de identidad.

Las políticas públicas deberán ofrecer una respuesta a los retos citados. Las personas y organizaciones, públicas y privadas, deberán gestionar la identidad en un entorno altamente complejo y distribuido. Además, habrá que garantizar el acceso autenticado, seguro e interoperable, a los complejos ecosistemas de información conectados.

La clave del cambio de paradigma reside en gestionar personas, en lugar de identidades separadas, implicar al usuario en el sistema de identidad electrónica y otorgarle el control de sus datos de identidad.

La evolución inmediata nos conduce a abordar el reto de la gestión de capacidades. Las personas deben poder hacer cosas en la Red: primero en el contexto de la Web 2.0 (orientado hacia la federación de redes sociales de personas) y luego en el de Red Semántica (orientado hacia la federación de redes sociales de máquinas). La legislación sobre la protección de datos deberá ampliarse para garantizar los derechos de las personas en este nuevo y prometedor escenario.

Bibliografía complementaria

ABC DE LA SIGNATURA ELECTRONICA. Ignacio Alamillo. Agencia Catalana de Certificación; Generalitat de Cataluña, 2005.

7 LAWS OF IDENTITY. THE CASE FOR PRIVACY-EMBEDDED LAWS OF IDENTITY IN THE DIGITAL AGE. Ann Cavoukian. Information and Privacy Commissioner of Ontario, 2006.

AT A CROSSROADS: 'PERSONHOOD' AND DIGITAL IDENTITY IN THE INFORMATION SOCIETY. Mary Rundle y otros. STI Working Paper 2007/7. Directorate for Science, Technology and Industry; OECD, 2008.

MAS ALLA DE LA DACTILOSCOPIA

Los sistemas de seguridad basados en rasgos anatómicos y de conducta ofrecen la mejor defensa contra la suplantación de identidad

Anil K. Jain y Sharath Pankanti

Para navegar entre las complejidades de la vida cotidiana, dependemos de un manojo de tarjetas y contraseñas que respaldan nuestra identidad. Pero perdamos la tarjeta bancaria, y el cajero automático se negará a darnos dinero. Si olvidamos una contraseña, nuestro propio ordenador no nos obedecerá. Si dejamos que nuestras tarjetas o contraseñas caigan en malas manos, las supuestas medidas de seguridad pueden convertirse en una herramienta para el fraude o la suplantación de identidad. La biometría (reconocimiento automático de personas mediante rasgos distintivos anatómicos o de conducta) ofrece la posibilidad de superar muchas de esas dificultades.

En comparación con un testigo físico (tarjeta bancaria) o un dato secreto (PIN), los rasgos biométricos son muchísimo más difíciles de falsificar, copiar, repetir, extraviar o adivinar. De hecho, ofrecen el único procedimiento para determinar si a una persona le han sido expedidos documentos oficiales (permiso de conducir, pasaporte, etcétera) bajo nombres distintos. Sin embargo, son muy fáciles de emplear como pruebas de identidad. Por todo ello, los sistemas biométricos han ido ganando adeptos en los últimos años. Ordenadores portátiles y teléfonos celulares que reconocen huellas dactilares se encuentran ya en el mercado. En algunos países, se emplea la seguridad biométrica para proteger artículos como tarjetas bancarias y pasaportes, determinar si una persona está autorizada para entrar en un edificio o comprobar que un individuo tiene derecho a cobrar las prestaciones sociales. Aunque esos sistemas distan de ser perfectos, con la incorporación de sensores baratos y potentes microprocesadores las técnicas biométricas se irán haciendo cada vez más omnipresentes.

Antropometría

El concepto de biometría no es nuevo. En 1879, Alphonse Bertillon, inspector de la policía francesa, propuso un complicado sistema de medidas corporales (longitud de brazos y pies, entre otras) para identificar a los delincuentes reincidentes. A lo largo del siguiente decenio, expertos británicos demostraron que la huella de cada dedo muestra un dibujo único e irrepetible que no cambia con el tiempo; ello sentó las bases para el desarrollo del sistema de clasificación de huellas digitales en 1896. Poco después, Scotland Yard empezó a recoger las huellas dactilares halladas en la escena del crimen para descubrir a los malhechores. En la actualidad, casi todas las instituciones encargadas de mantener el orden público se basan en la dactiloscopia para identificar delincuentes, resolver crímenes y comprobar los antecedentes de los aspirantes a puestos de trabajo delicados.

CONCEPTOS BASICOS

- Los sistemas de identificación biométrica son difíciles de burlar y más sencillos de emplear que los sistemas de seguridad tradicionales basados en tarjetas de identidad y contraseñas.
- Las técnicas biométricas están en expansión gracias a la disponibilidad de microprocesadores potentes y baratos.
- Para que esos sistemas alcancen todo su potencial, deberá aumentarse su eficacia mediante la reducción de las tasas de error.



ABRETE SESAMO: Para aumentar la precisión, algunos sistemas de seguridad examinan varios rasgos biométricos.

BIOMETRIA EN ACCION

- Los estados miembro de la Unión Europea deben empezar a emitir pasaportes con datos biométricos en el verano de 2009.
- Algunas cafeterías de institutos de enseñanza secundaria estadounidenses han establecido un sistema de pago sin efectivo basado en las huellas dactilares.
- En fecha reciente, un equipo encabezado por Lockheed-Martin ganó un contrato de 10 años con el FBI por un valor de 10.000 millones de dólares para desarrollar un sistema de identificación que incorpora técnicas biométricas (reconocimiento de cara, iris y palma de la mano).
- La Oficina de Administración de Personal de la ciudad de Nueva York tiene un contrato de 181,1 millones de dólares con Science Aplications International, de San Diego, para instalar un reloj de control biométrico que escanea los dedos y la palma de la mano del trabajador que ficha.
- El ordenador portátil Protégé M800 de Toshiba se vende con un programa de reconocimiento de rostro y un lector de huellas digitales opcional.

Pero no se utilizan sólo las huellas dactilares. Los sistemas de identificación incorporan también otras características físicas o de conducta, por separado o en grupo. La prioridad actual en biometría es diseñar un dispositivo totalmente automático, ultrarrápido, preciso, de uso cómodo y económico, que pueda insertarse en los sistemas de seguridad existentes. Además de los dactiloscópicos, en los últimos treinta años los especialistas han desarrollado sistemas de identificación basados en otros rasgos: la cara, las manos, la voz y el iris (la parte coloreada del ojo).

Los rasgos sobre los que operan los sistemas biométricos deben cumplir dos requisitos: ser exclusivos de cada individuo y no cambiar con el tiempo; algunos redundan en una precisión exquisita, otros en una mayor viabilidad o menor coste. En función de los objetivos del sistema de identificación, se utilizará un rasgo u otro; no hay ninguno que por sí solo sea óptimo para todas las aplicaciones.

Consideremos los tres rasgos anatómicos de uso más frecuente: las huellas dactilares, el rostro y el iris. Además de su empleo en criminología, la dactiloscopia constituye la base de los sistemas automáticos de control fronterizo en numerosos países. El programa US-VISIT del Departamento de Seguridad Interior estadounidense ha procesado más de 75 millones de visitantes desde su puesta en servicio en 2004. Desde una perspectiva comercial, una de las mayores ventajas del uso biométrico de las huellas dactilares es que los sensores para captar las huellas son baratos (cuestan unos 2 euros) y de tamaño reducido, lo que permite incorporarlos a productos de consumo como ordenadores portátiles, teléfonos celulares e

KEVIN HAND (*ilustración*); TOSHIBA, SINGAPUR (*ordenador portátil*)

RASGOS BIOMETRICOS

El rasgo o rasgos biométricos que se elijan para emplear en un sistema de seguridad depende de la aplicación. En la tabla que sigue se resumen los puntos fuertes y flacos de cada uno de los cuatro identificadores biométricos más comunes. Los expertos coinciden en que, en un sistema de autenticación biométrica ideal, las tasas de "aceptaciones falsas" (aceptaciones de patrones no coincidentes) y "rechazos falsos" (rechazos de patrones coincidentes) deben ser inferiores al 0,1 por ciento. Sin embargo, ensayos realizados en el Instituto Nacional de Normalización y Tecnología estadounidense han demostrado que ninguno de los sistemas cumple esa exigencia.

Propiedad	Rasgos biométricos: Huella dactilar	Rostro	Iris	Voz
Discriminabilidad	Alta	Baja	Alta	Baja
Permanencia	Alta	Media	Alta	Baja
Facilidad de detección	Media	Alta	Media	Media
Celeridad y rendimiento económico	Alta	Baja	Alta	Baja
Aceptación por el público	Media	Alta	Baja	Alta
Dificultad de falseamiento	Alta	Baja	Alta	Baja
Tasa de rechazos falsos*	0,4 %	1,0–2,5 %	1,1–1,4 %	5–10 %
Tasa de aceptaciones falsas*	0,1 %	0,1 %	0,1 %	2–5 %

* *Las tasas de error dependen de las condiciones del ensayo, los sensores empleados y la población estudiada.*

incluso lápices de memoria. Sin embargo, esos sensores compactos presentan unas tasas de error superiores a las de sus parientes de mayor tamaño y precio utilizados en la lucha contra la delincuencia, pues escanean una fracción menor del dedo y la imagen que registran es de menor calidad.

El reconocimiento facial está ganando aceptación como rasgo de seguridad para ordenadores y teléfonos celulares, en parte porque aprovecha las cámaras que llevan incorporadas la mayoría de esos aparatos. Los sistemas de identificación basados en el reconocimiento facial son muy precisos cuando las imágenes se captan en condiciones controladas (el sujeto mirando hacia delante, luz interior y una expresión facial neutra, por ejemplo); pero fallan cuando la imagen original y la nueva difieren a causa de un cambio de postura, iluminación, expresión, edad, presencia de gafas, barba, etcétera. Esa sensibilidad a variaciones tan habituales resulta problemática sobre todo para la vídeo-vigilancia, ya que los sujetos no se presentan frente a la cámara en unas posturas predeterminadas. Quizás en el próximo decenio la técnica habrá avanzado lo suficiente para desarrollar una vídeo-vigilancia por contraste facial totalmente automática y en tiempo real.

En lo que respecta al iris (cuyo dibujo complejo y texturado se cree que es único en cada persona y permanente), el reconocimiento se realiza con gran precisión y rapidez. El sujeto se limita a mirar hacia el interior de un escáner durante unos segundos; la imagen así captada se analiza y se registra. La compro-

LUCY READING-IKKANDA

bación se efectúa mediante la comparación de la secuencia de bits del individuo con las secuencias almacenadas en una base de datos. La celeridad y precisión de este método han impulsado el desarrollo de sistemas de identificación a gran escala basados en el iris, como el Sistema de Reconocimiento del Iris para Inmigración (IRIS, de "Iris Recognition Immigration System"), del Reino Unido. Los pasajeros inscritos en la base de datos del IRIS pueden eludir los trámites habituales de inmigración en el aeropuerto, reduciendo así el tiempo de espera previo al viaje.

No obstante, el reconocimiento del iris tiene sus inconvenientes. El método depende, por ejemplo, del uso de algoritmos que representan los dibujos aleatorios del iris en forma de secuencia de bits (ningún experto humano puede determinar si las imágenes de dos iris coinciden). Por ello, los datos iridiológicos no se aceptan como pruebas judiciales.

Contrastes imperfectos

El desarrollo de sistemas biométricos se enfrenta asimismo a otras dificultades. A diferencia de los sistemas de identificación que requieren una contraseña o un testigo físico, los sistemas biométricos deben tomar las decisiones basándose en contrastes imperfectos. Todo sistema de comparación da errores de dos tipos básicos: la "aceptación falsa" (da por bueno el contraste entre el patrón entrante y uno contenido en la base de datos, que en realidad no coincide con aquél) y el "rechazo falso" (declara fallado el contraste entre el patrón entrante y uno contenido en la base de datos que en realidad coincide con aquél).

Según los expertos, las tasas de aceptaciones falsas y de rechazos falsos no deberían exceder el 0,1 por ciento (un error cada 1000 coincidencias declaradas y un error cada 1000 no coincidencias declaradas). Pero en las evaluaciones realizadas por el Instituto Nacional de Normalización y Tecnología estadounidense entre 2003 y 2006, las tasas de error de sistemas basados en las huellas dactilares, el rostro, el iris y la voz (otro rasgo biométrico comúnmente usado) sobrepasaron todas el 0,1 por ciento.

Aumentar el umbral de exigencia para las coincidencias rebaja la tasa de aceptaciones falsas, pero a costa de aumentar los rechazos falsos. Reducir ambas tasas a la vez requiere desarrollar sensores biométricos que generen imágenes de alta calidad y depurar los extractores y comparadores de rasgos. El sistema también deberá asegurarse contra el sabotaje: debe impedirse que los datos biométricos sean interceptados y reinsertados en el sistema. Y debería ser imposible hurgar en los ordenadores y programas informáticos empleados en el análisis biométrico. Por suerte, al ser estos ataques comunes a todos los sistemas de autenticación, incluidas las variedades de contraseña y de testigo, pueden contrarrestarse con las herramientas habituales. La criptografía, por ejemplo, impide que los piratas informáticos intercepten, reproduzcan o alteren la información.

Más arduo es diseñar un sistema biométrico seguro, que acepte sólo los rasgos legitimados por la presencia de su poseedor, sin que pueda ser burlado por unos rasgos amañados o falsificados (la copia en plástico del dedo de una persona, por ejemplo). A tal fin, sensores que detecten el calor y otros signos vitales ayudan a garantizar que la entrada que se quiere comparar no procede de un objeto inanimado.

Pero acaso la estrategia más eficaz para mejorar la precisión, fiabilidad y seguridad de la biometría sea la detección de múltiples rasgos biométricos o varias muestras de un rasgo (más de una huella dactilar, por ejemplo). Reafirmar la identidad de un sujeto mediante esas combinaciones ofrece una prueba cada vez más irrefutable de que los datos biométricos los está presentando la persona auténtica y no un impostor. De hecho, numerosos sistemas de pasaporte están evolucionando por ese camino. El programa US-VISIT, que escaneaba sólo dos dedos de los ciudadanos no estadounidenses, ha empezado a recoger información de los diez dedos; en el futuro, el sistema comprobará huellas dactilares y rostros a la vez.

El laberinto de la privacidad

El uso de la biometría plantea ciertas cuestiones sobre la privacidad. ¿De quién son los datos, de la persona o del proveedor del servicio? ¿Se emplearán esos datos para fines no pretendidos, como deducir aspectos de la salud de un individuo, por ejemplo? Los dispositivos del futuro funcionarán probablemente con discreción, captando rasgos biométricos sin la intervención activa del usuario. Tal furtividad introduce más confusión en la cuestión de la privacidad.

A día de hoy no vemos todavía soluciones concretas y viables para abordar todo el espectro de amenazas a la privacidad. Creemos, sin embargo, que esos problemas pueden resolverse mediante debates públicos y medidas políticas. Así tendrá que ser. Es sólo cuestión de tiempo que los continuos avances en las técnicas biométricas las sitúen en el centro de la escena, en un esfuerzo para combatir los cada vez mayores problemas de seguridad y fraudes de identidad a los que se enfrenta nuestra sociedad.

Los autores

Anil K. Jain es profesor de los departamentos de informática e ingeniería, ingeniería eléctrica e informática, y probabilidad y estadística en la Universidad estatal de Michigan. **Sharath Pankanti** dirige el grupo de visión por computador del Centro de Investigación Thomas J. Watson, de Yorktown Heigths (Nueva York). Centra su trabajo en el desarrollo de sistemas de reconocimiento de objetos. Ambos poseen numerosas patentes relacionadas con la dactiloscopia.

Bibliografía complementaria

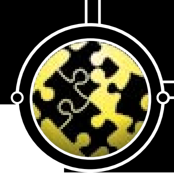
BIOMETRIC RECOGNITION: SECURITY AND PRIVACY CONCERNS. S. Prabhakar, S. Pankanti y A. K. Jaim en *IEEE Security & Privacy*, vol 1, n.º 2, págs. 33-42; marzo/abril 2003.

BIOMETRIC SYSTEMS: TECHNOLOGY, DESIGN AND PERFORMANCE EVALUATION. Dirigido por J. Wayman, A. K. Jain, D. Maltoni y D. Maio. Springer, 2005.

HANDBOOK OF MULTIBIOMETRICS. A. Ross, K. Nandakumar y A. K. Jain. Springer 2006.

PROBING THE UNIQUENESS AND RANDOMNESS OF IRISCODES: RESULTS FROM 200 BILLION IRIS PAIR COMPARISONS. John Daugman en *Proceedings of the IEEE*, vol. 94, n.º 11, págs. 1927-1935; 2006.

HANDBOOK OF BIOMETRICS. Dirigido por A. K. Jain, P. Flynn y A. Ross. Springer 2007.



COTEJO DE INFORMACIONES

FUSION DE BASES DE DATOS

Integrar toda la información personal, desde la factura de la tarjeta de crédito hasta la lista de llamadas de teléfono móvil, en una carpeta digital omnisciente, propio de una pesadilla de George Orwell, no es hazaña fácil

Simson L. Garfinkel

CONCEPTOS BASICOS



- La idea de intercomunicar bases de datos, técnica denominada fusión de datos, es la bestia negra de los defensores de la privacidad. Sin embargo, hasta el momento no se aplica excepto en determinados contextos (los casinos) o para localizar a padres que no tienen la custodia de sus hijos y que no están al día en el pago de la pensión correspondiente.
- La fusión de datos supone un desafío técnico porque las bases de datos están repletas de errores y coincidencias sin trascendencia. Los nuevos algoritmos desarrollados suponen una mejora sustantiva, pero ¿consiguen inclinar la balanza de costes y beneficios del lado de éstos?

Hace unos años tomé un café en una cantina de camino al aeropuerto de San Francisco; lo pagué con la tarjeta. Dejé el coche en el parking de la terminal y subí a un avión, rumbo al Reino Unido. Ocho horas más tarde llegué a Heathrow, compré una tarjeta prepago para el teléfono móvil y al ir a sacar un billete de tren que me llevara a Londres, mi tarjeta de crédito dejó de funcionar. No pude abonar el billete.

No descubrí lo que había pasado hasta que volví a los Estados Unidos. Al parecer, el café de la cantina, sumado a la tarjeta prepago en el extranjero, había activado un algoritmo antifraude en el sistema informático de la compañía de mi tarjeta de crédito. El sistema intentó localizarme por teléfono y al dar con el contestador automático, anuló directamente mi tarjeta de crédito.

Lo que más me molestó de todo el incidente fue que el sistema informático debería haberse dado cuenta de que era yo quien estaba usando la tarjeta de crédito en Inglaterra. Después de todo, había comprado el billete de avión con la misma tarjeta y había volado con una de las principales compañías aéreas. ¿No se supone que todas esas bases de datos están intercomunicadas?

Casi todo el mundo piensa que lo están. Gracias al cine americano y películas como *Enemigo público* o la trilogía de Jason Bourne, pensamos que determinadas agencias secretas tienen acceso instantáneo a todas las bases de datos y pueden saberlo todo sobre nosotros en cualquier momento. El proceso de acceder a información de varias fuentes y combinarla, proceso denominado fusión de datos, tiene por objetivo crear una fuente de información más poderosa, flexible y precisa que las fuentes originales.

Los partidarios de la fusión de datos creen que su desarrollo permitiría a las organizaciones hacer un mejor uso de la información de la que ya disponen, mientras que los detractores sostienen que la fusión de datos amenaza nuestra libertad personal, al darle a la información personal un uso distinto del original para el que en un principió se tomó. Ambas partes arrancan del supuesto de que la fusión de datos funciona. La verdad es que los sistemas no se han desarrollado tanto, ni son tan omniscientes ni fiables como podríamos imaginar.

E pluribus unum

La técnica de fusión de datos tiene sus orígenes en la época de los programas de rastreo informáticos de los años setenta. Cuando el Congreso estadounidense aprobó la ley federal de privacidad en 1974, autorizó también la creación del Servicio Federal de Localización de Padres, que mantiene actualizada una larga lista negra que impide el acceso a numerosos



1. COLECCION DE DOCUMENTOS de identidad, pasaportes, permisos de conducir, recibos, facturas... unidos entre sí para mostrar las posibles relaciones entre las bases de datos.

MELISSA THOMAS (*fotoilustración*); PATRIK STOLLARZ *Getty Images* (*teléfono*); THINKSTOCK/CORBIS (*tarjeta de registro de libro*); JIM CRAGMYLE *Corbis* (*dispositivo en ordenador portátil*); ELISE AMENDOLA *AP Photo* (*permiso de conducir*); PURESTOCK (*pasaporte*); DAVID MACK *Photo Researchers, Inc.* (*ADN*); PHILIP JAMES CORWIN *Corbis* (*extracto de cuenta*); SHEILA TERRY *Photo Researchers, Inc.* (*disco duro*)

servicios federales, como el pasaporte, a padres que no tienen la custodia de sus hijos y no están al día en el pago de la pensión correspondiente. Estos datos están fusionados con los del Registro Nacional de Nuevos Contratos Laborales para detectar a los nuevos empleados que son padres y que no están al día en los pagos, con el fin de confiscarles el salario.

La expresión técnica "fusión de datos" se acuñó en 1984, cuando investigadores del Centro de Tecnología Avanzada de Lockheed Martin publicaron dos artículos sobre un sistema de "fusión de datos tácticos". El sistema descrito fusionaba en tiempo real información del campo de batalla, proveniente de sensores, bases de datos y otras fuentes, para su análisis por seres humanos. Desde entonces, la idea ha florecido. Los investigadores de bioinformática hablan de fusión de datos genómicos. El Departamento de Seguridad Nacional norteamericano ha gastado más de 250 millones de dólares en la creación de 58 centros de fusión de datos de ámbito estatal y local. Nielsen, empresa dedicada a la mercadotecnia, ha desarrollado técnicas de fusión de datos para identificar y dirigirse a clientes potenciales con características específicas, en lugar de derrochar dinero en el enfoque aleatorio de la mercadotecnia tradicional.

Si bien la fusión de datos se puede tratar desde muchos puntos de vista, su uso en la identificación de potenciales terroristas es el que ha suscitado un mayor debate. "La clave para la detección de terroristas es buscar patrones de actividad propios de los planes terroristas, basándose en la observación de otros grupos de terroristas activos y en el análisis de atentados pasados", escribieron en 2006 el contraalmirante John Poindexter y Robert L. Popp, de la Agencia de Proyectos de Investigación Avanzada para la Defensa. Afirmaban que la explosión del World Trade Center de 1993 y el atentado de Oklahoma City de 1995 podrían haberse evitado si el gobierno hubiera podido acceder a bases de datos comerciales para detectar compras de gran cantidad de fertilizantes por parte de personas que no fueran agricultores. Sin embargo, obtener los datos relativos a las compras y compararlos con una base de datos de empleo y de propietarios de terrenos de cultivo habría requerido un acceso sin precedentes del gobierno a sistemas informáticos privados. Cada transacción —y, por tanto, cada ciudadano— habría sido controlada sin indicios razonables de culpabilidad. Por estas y otras razones el Congreso anuló en 2003 el programa de investigación de Poindexter

FUSION Y CONFUSION

Para saber cuánta información sobre nosotros circula por ahí, uno de los redactores de la revista compró a una agencia de venta de bases de datos un informe sobre sus datos personales, incluyendo datos penales, de propiedad inmobiliaria e inclusión en listas de morosos. El documento contenía numerosos errores (faltas de ortografía y confusión con otras personas con el mismo nombre en otras partes del país, muchas de las cuales tenían embargados sus bienes, aunque, afortunadamente, ninguna de ellas con antecedentes penales). El informe no mostró signos de robo de identidad. Por supuesto, no todo el mundo tiene tanta suerte.

El juego de los jugadores

Los casinos de Las Vegas fueron los pioneros en la fusión de datos de diferentes fuentes, porque se enfrentan a las técnicas más variadas de intentar arruinarlos. Reseño varios ejemplos basados en historias reales.



KENN BROWN *Mondolithic Studios*

y Popp, un proyecto llamado Conocimiento Total de la Información.

Océanos de datos

El secretismo del gobierno no ayuda a disipar los temores de los defensores de las libertades civiles. Las agencias públicas han revelado poca información acerca de los sistemas de fusión de datos que pueden o no haber desarrollado para proteger la seguridad nacional: las agencias sostienen que, para los "malos", sería más fácil eludir los programas de fusión de datos si supieran cómo funcionan. Sin embargo, la información disponible induce a pensar que la fusión de datos supone algo más que problemas éticos y jurídicos; plantea también dificultades técnicas.

La calidad de los datos es una de esas dificultades. Gran parte de la información de las bases de datos se recopiló en un principio para fines estadísticos exclusivamente y puede que no sea lo bastante fiable para tomar decisiones de forma automática que puedan tener resultados punitivos. En 1994, Roger Clarke, de la Universidad Nacional de Australia en Canberra, estudió programas de concordancia usados por los gobiernos federal y estatal de los Estados Unidos y Australia. Estos sistemas analizaron millones de campos de datos y señalaron miles de resultados positivos. Sin embargo, la mayoría resultaron ser falsos positivos. Por ejemplo, un programa para detectar fraudes en el sistema de la seguridad social comparó los registros de empleo del Departamento de Salud y Servicios Asistenciales con los subsidios pagados en los condados cercanos a Washington DC. El programa generó alrededor de 1000 resultados positivos, pero las investigaciones posteriores demostraron que tres cuartas partes de las personas identificadas eran inocentes. El beneficio producido no justificaba el coste de recogida de datos, formación del personal y depuración de los falsos positivos.

Muchos opinan que, si un programa de fusión pudiera prever y evitar un atentado terrorista, valdría la pena desarrollarlo a cualquier precio. Poindexter, marino de profesión, comparaba el desafío técnico a encontrar un submarino enemigo en la inmensidad del océano. Pero descubrir señales de planes terroristas en un océano de datos es mucho más difícil que encontrar submarinos en un océano de agua. Los océanos del planeta son muy gran-

DATOS OCULTOS

Los documentos creados con procesadores de texto y otros archivos informáticos contienen "metadatos" ocultos (fecha de creación del documento, su nombre, tipo de ordenador, hojas de estilo de formato e incluso partes suprimidas, comentarios sarcásticos, etcétera). Esta información es un tesoro para detectives y periodistas de investigación.

Nuestra redacción analizó los borradores de este artículo de Simson Garfinkel por medio de dos herramientas gratuitas de análisis de metadatos. Gracias a ello, descubrimos que los había creado usando OpenOffice en un ordenador con Windows XP, y disfrutamos leyendo comentarios semiocultos que había escrito para sí mismo. Uno de los borradores era la versión número 139 y había supuesto 330 minutos de tiempo de edición. Estos datos nos confirmaron que nuestro autor trabajó duramente.

des, pero cada punto puede identificarse de forma unívoca mediante una latitud, una longitud y una profundidad. Los océanos de datos no admiten identificaciones tan claras. Por otra parte, el tamaño de los océanos de agua no se duplica cada pocos años, el de los datos sí. Gran parte del espacio de la información no está registrado; los datos se hallan distribuidos en millones de sistemas informáticos, muchos de ellos escondidos o al menos desconocidos para las autoridades.

La fusión es complicada porque nos ahogamos en datos de una multitud de fuentes, todas con diferentes niveles de detalle e incertidumbre. El verdadero desafío de la fusión de datos no está en conseguir los datos, sino en interpretarlos correctamente.

¿Qué hay en los discos duros?

Una buena manera de entender las complicaciones de la fusión de datos es empezar con la información del disco duro de nuestro propio ordenador. Eso es exactamente lo que hice entre 1998 y 2005: compré más de 1000 discos duros de segunda mano en eBay, en pequeñas tiendas de informática y en rastrillos; incluso recogí algunos ordenadores abandonados en la calle. En enero de 2003, Abhi Shelat, hoy contratado por la Universidad de Virginia, y yo publicamos un artículo describiendo lo que encontramos.

Alrededor de un tercio de las unidades ya no funcionaban y otro tercio había sido adecuadamente formateado antes de desecharlas. El tercio restante era toda una fuente de información personal: mensajes de correo electrónico, informes, datos financieros... Un disco duro provenía de un cajero automático y tenía miles de números de tarjetas de crédito. Otro había sido utilizado por un supermercado para enviar al banco la información relativa de los pagos con tarjeta de crédito. Ninguna de ambas unidades se formateó correctamente antes de su reventa.

Las herramientas que me permitieron bucear en los discos duros están al alcance de cualquiera y no son especialmente complejas. Los departamentos de policía de todo el mundo utilizan el mismo tipo de herramientas para recuperar archivos de ordenadores y teléfonos móviles. A veces los datos se encuentran ocultos en documentos visibles. Tenemos por ejemplo el caso de Dennis Rader, el llamado asesino BTK, que cometió ocho asesinatos en Wichita, Kansas, en los años setenta y ochenta, y luego pasó a la clandestinidad. El asesino reapareció en marzo de 2004; remitió una carta al periódico Wichita Eagle en la que detallaba los crímenes de su pasado y adjuntaba un disquete que incluía una carta a una cadena

Cómo funciona la fusión de datos

Un algoritmo de fusión de bases de datos, creado para los casinos, ilustra las dificultades de la fusión de datos y cómo pueden superarse.

Fuente A (2002)
Marc R Smith
123 Main St
(713) 555 5769
SS: 444-44-4444
DL: 1133P107A

Fuente B (2003)
Randal Smith
DOB: 06/17/1934
(713) 555 5577

Un documento de identidad y una entrada de directorio telefónico contienen información diferente, por lo que el sistema da por supuesto de momento que representan a dos personas distintas.

Fuente A (2002)
Marc R Smith
123 Main St
(713) 555 5769
SS: 444-44-4444
DL: 1133P107A

Fuente B (2003)
Randal Smith
DOB: 06/17/1934
(713) 555 5577

Fuente C (2004)
Marc Randy Smith
456 First Street
(713) 555 5577
DL: 1133P107A

Un tercer paquete de información contiene información común a los dos registros originales: el número de identidad del primero y el número de teléfono del segundo. Por lo tanto, el sistema asigna ahora los tres a la misma persona.



Fuente A (2002)
Marc R Smith

Fuente B (2003)
Randal Smith
DOB: 06/17/1934

Fuente C (2004)
Marc Randy Smith
456 First Street
(713) 555 5577
DL: 1133P107A

Fuente D (2005)
Randy Smith Sr.
DOB: 06/17/1934
(713) 555 5577
SS: 777-77-7777

Fuente A (2002)
Marc R Smith

Fuente C (2004)
Marc Randy Smith
456 First Street
(713) 555 5577
DL: 1133P107A

Fuente B (2003)
Randal Smith
DOB: 06/17/1934

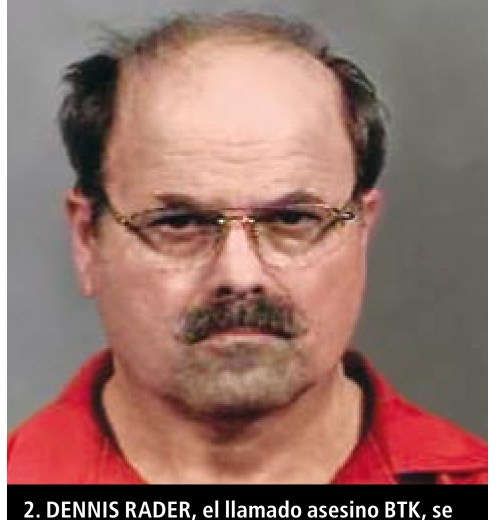
Fuente D (2005)
Randy Smith Sr.
DOB: 06/17/1934
(713) 555 5577
SS: 777-77-7777

Un cuarto elemento de información, sin embargo, contiene una fecha de nacimiento diferente, lo que indica que los registros anteriores representan en realidad a dos personas, padre e hijo, que comparten el apellido y la dirección.

MELISSA THOMAS

El autor

Simson L. Garfinkel trabaja en el mundo académico, el periodismo y la industria. Es un experto informático de la Escuela Naval de Posgrado en Monterrey, California. Su libro de texto sobre seguridad informática, escrito conjuntamente con Gene Spafford, ha sido traducido a más de una docena de idiomas. Ha fundado una empresa de seguridad informática y registrado varias patentes. Las opiniones expresadas en este artículo representan la opinión del autor y no las del gobierno de los EE.UU.



2. DENNIS RADER, el llamado asesino BTK, se delató inintencionadamente al enviar a una cadena de televisión un archivo de Microsoft Word con metadatos ocultos.



3. LOS EVACUADOS por el huracán Katrina, en la imagen en el Astródomo de Houston, pudieron reunirse con sus familias gracias a un sencillo sistema de fusión de datos.

ROBO DE IDENTIDAD

Muchos de quienes trabajan en *Scientific American* han sufrido diversas formas, no demasiado graves, de robo de la identidad. Con todo, los problemas pudieron domeñarse porque las bases de datos permanecían aisladas entre sí. Mas a medida que las empresas las van enlazando, el ladrón de un fragmento de información podría terminar por arruinar la identidad digital de otra persona.

- El banco de uno de ellos anuló recientemente su tarjeta de crédito tras detectar algunas operaciones poco habituales. Algunas eran correctas, pero dos resultaron fraudulentas. El banco canceló la tarjeta y envió una nueva. Sigue siendo un misterio quién robó su número de tarjeta de crédito.

- Otro recibió una notificación de confirmación de cambio de señas por parte de sus agentes de bolsa. La nueva dirección no era correcta. El corredor, que era nuevo en la empresa, declaró no saber nada, por lo que este miembro del personal de *Scientific American* llamó a la policía. La empresa descubrió que el corredor buscaba cuentas con poca actividad y transfería los fondos a un cómplice.

- Otro comenzó a recibir avisos de impago por parte de su proveedor de telefonía móvil. Resultó evidente que alguien había abierto una cuenta con su nombre. Le llevó un año resolver el problema y salir de la lista de morosos.

de televisión local. En el archivo de Microsoft Word del disco había "metadatos" que hacían referencia a un ordenador de una iglesia. La policía fue a la iglesia y descubrió que la persona que había utilizado el ordenador para escribir la carta era el presidente del consejo de la congregación. Era el asesino.

Hash

Averiguar qué documentos son importantes y cuáles no es difícil y requiere relacionar la información del disco duro con información externa. Cuando empecé a analizar los discos duros en la década de los noventa, encontré en muchos de ellos copias de un periódico, *Island Hopper News*. Resultaba sospechoso. Luego me enteré de que este periódico electrónico es en realidad un archivo de demostración distribuido por Microsoft con el programa Visual Studio 6.0. Si no lo hubiese sabido, podría haber extraído conclusiones erróneas sobre los antiguos propietarios de los discos duros.

El único modo de descartar archivos inocuos es muestrear el mundo de los documentos digitales y crear una lista de los que se han difundido mucho. Un método rápido y automático de hacerlo es crear un conjunto *hash*. Los algoritmos criptográficos *hash* pueden asignar un *hash* o huella digital electrónica única a cualquier archivo digital. Dos de los algoritmos más populares son MD5, que crea una huella digital de 128 bits, y SHA-1, que genera una huella digital de 160 bits de longitud. Gracias a este sistema, en lugar de comparar dos ficheros byte por byte, el análisis puede examinar sus huellas digitales. Es exactamente lo que hacen muchas herramientas utilizadas en la técnica forense.

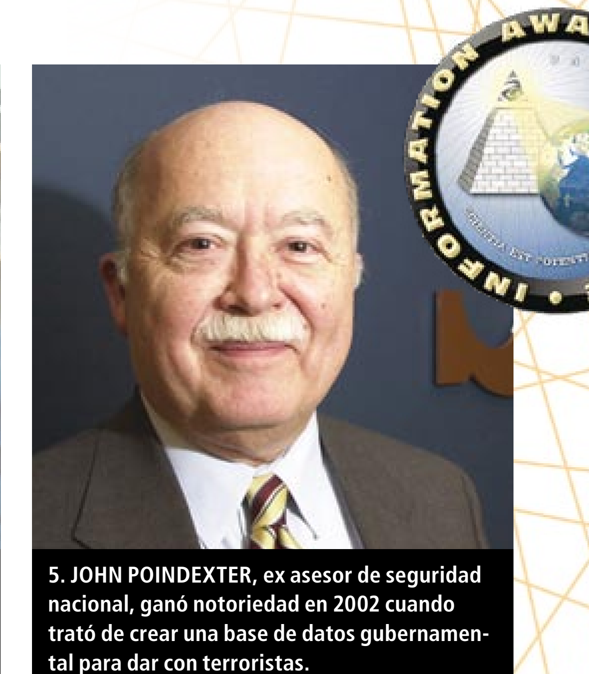
La Biblioteca Nacional de Referencia de Programas Informáticos del Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST) recibe financiación del Departamento de Justicia para que adquiera programas de cientos de editores y calcule la función *hash* criptográfica de todos los archivos. El NIST distribuye posteriormente la correspondiente base de datos, que cuenta actualmente con más de 46 millones de entradas, para facilitar a los investigadores forenses un mecanismo rápido y fiable de filtrar los archivos que han sido distribuidos por los editores de programas, como el mencionado *Island Hopper News* y que, por tanto, se pueden ignorar. Hay bases de datos disponibles de otras agencias federales estadounidenses que incluyen las huellas digitales de herramientas para piratas informáticos y de pornografía infantil.

A pesar de su utilidad, las bases de datos *hash* representan sólo una pequeña muestra de todos los documentos que circulan. Para complementarlas, he desarrollado una técnica llamada análisis cruzado. Esta herramienta agrupa automáticamente información dispersa en miles de unidades de disco duro, memorias USB y otras fuentes de datos. La técnica permite detectar y seleccionar identificadores tales como direcciones de correo electrónico y números de tarjetas de crédito; los clasifica de acuerdo a la frecuencia con la que aparecen: cuanto más común es un identificador, menos importante, cabe suponer, es. Por último, la herramienta correlaciona los identificadores entre todas las unidades de memoria: si una dirección de correo electrónico o número de tarjeta de crédito aparece en sólo dos unidades de disco entre miles, hay una probabilidad

AP PHOTO (*Rader*); DAVID PORTNOY *Getty Images (víctimas del Katrina)*; CORTESIA DE SIMSON L. GARFINKEL (*Garfinkel*); ALEX BRANDON *AP Photo (Poindexter)*; DEPARTAMENTO DE DEFENSA DE EE.UU. (*logo*)



4. EL AUTOR analizó el contenido de discos duros abandonados para ver cómo podría la fusión de datos ayudar en las investigaciones forenses.



5. JOHN POINDEXTER, ex asesor de seguridad nacional, ganó notoriedad en 2002 cuando trató de crear una base de datos gubernamental para dar con terroristas.

elevada de que estas dos unidades guarden mutua relación.

Resolución de identidades

Otro problema para los usuarios de la fusión de datos es la identidad. En el mundo electrónico puede haber decenas de personas que comparten el mismo nombre y una persona que utiliza decenas de nombres. Por ejemplo, una base de datos puede registrar a Poindexter como John Marlan Poindexter o J. M. Poindexter, o incluso almacenar con una falta de ortografía el apellido del contraalmirante Pointexter. El nombre de una persona puede figurar en una base de datos como Juan Manuel, en otra como Juan M. y en una tercera como J. Manuel. Una persona cuyo nombre árabe se transcriba Haj Imhemed Otmane Abderaqib en Africa Occidental, podría ser conocida en Iraq como Hajj Mohamed Abd Al Uthman Ragib.

La resolución de identidades consiste en identificar los nombres y números de cuenta que existen en el mundo electrónico con cada ser humano que habita el planeta. Sin resolución de identidades, no puede haber fusión de datos. Curiosamente, los casinos de Las Vegas han desarrollado gran parte de las técnicas existentes de resolución de identidades. En virtud de la ley de Nevada, los casinos están obligados a denegar la entrada a los jugadores que hayan declarado que tienen un problema con el juego. Dichos jugadores se inscriben voluntariamente en una lista para que no se les deje jugar más. Pero el juego puede ser una enfermedad, y algunas personas inscritas en la lista tratan de colarse en los casinos cambiándose el nombre o modificando ligeramente su fecha de nacimiento. Los casinos también persiguen impedir la entrada a los sospechosos o condenados por hacer trampas. Por último, a los casinos les interesa saber si un jugador que está ganando grandes sumas en la mesa de blackjack es pariente o compañero de piso del crupier.

Como consecuencia, los casinos han costeado el desarrollo de una técnica llamada análisis de relaciones no obvias (NORA, por sus siglas en inglés), que combina la resolución de identidades con las bases de datos de instituciones crediticias, con registros públicos y con estancias en hoteles. Un sistema NORA, por ejemplo, podría descubrir que la esposa del crupier de blackjack vivió una temporada en el mismo edificio que el jugador que acaba de ganar 100.000 dólares.

En los años noventa, el programador Jeff Jonas desarrolló un sistema que relacionaba los nombres del sistema informático de un casino con otras fuentes de información. El sistema tiene en cuenta los posibles errores, la ambigüedad y la incertidumbre. El programa funciona mediante la construcción de hipótesis basadas en datos y la revisión de estas hipótesis cuando se dispone de nuevos datos. Supongamos que insertamos el número de la Seguridad Social de un tal Marc R. Smith, un informe sobre Randal Smith, que solicitó un crédito, y una solicitud de crédito de Marc Randy Smith. El programa puede imaginar que todos estos nombres pertenecen a la misma persona, sobre todo si Marc R. Smith y Marc Randy Smith tienen el mismo número de la Seguridad Social y si Randal Smith y Marc Randy Smith tienen el mismo número de teléfono.

Pero supongamos que llega más información, y que indica que Randal Smith nació

en 1974, mientras que Randy Smith nació en 1934. Ahora el sistema descarta su conclusión anterior y establece que Randal Smith es realmente Randal Smith, padre, mientras que Randy Smith es Randy Smith, hijo. La clave es programar el sistema de manera que nunca confunda datos originales con conclusiones deducidas de dichos datos.

Jonas vendió el sistema junto con la empresa a IBM en 2005. Desde entonces, IBM ha añadido una característica llamada resolución de identidades anónima: con ella dos organizaciones pueden verificar si comparten el nombre de una persona en sus respectivas bases de datos sin compartir los nombres de las personas que no coincidan. La técnica funciona comparando *hash* criptográficos, en vez de nombres reales.

Los defensores de la privacidad sostienen que los *hash*, el análisis cruzado, la resolución de identidades y demás técnicas no ayudan mucho para vencer sus reticencias. Después de todo, estos sistemas siguen usando datos personales para fines distintos de aquellos para los que se tomaron originalmente. También hacen barridos de información sobre multitud de ciudadanos independientemente de que las personas involucradas sean sospechosas o no de haber cometido un delito. Sin embargo, los sistemas actuales generan un número de falsos positivos significativamente menor que los desarrollados en el decenio de los ochenta. En algún momento, el beneficio obtenido por la sociedad puede llegar a superar el precio a pagar en términos de privacidad por tener ordenadores que fisgan en los datos de todo el mundo.

Conclusiones

¿Hasta que punto son eficientes los sistemas de fusión de datos? La calidad de los datos sigue siendo un serio problema. Por ejemplo, pruebe a pedir su propio informe de riesgo crediticio a las tres mayores agencias de riesgo crediticio de Estados Unidos. Probablemente, cada informe contendrá errores e incoherencias. Estos datos pueden permanecer inactivos durante años sin causar problemas. El problema surge cuando algún algoritmo de nuevo cuño le da demasiada importancia a esas pequeñas contradicciones.

Aunque los datos fueran fiables, descubrir coincidencias cuando se comparan bases de datos puede tener un significado real o puede ser puramente casual. Es algo inevitable, tanto como encontrar dos personas en una habitación con la misma fecha de cumpleaños. Quizá cuatro personas sospechosas que se reúnen una vez por semana y hacen un largo viaje en coche estén planeando un crimen. Por otra parte, tal vez sólo pertenecen al mismo equipo de fútbol y viajan juntos para jugar el partido de cada semana.

Las expectativas respecto a la fusión de datos pueden ser poco realistas. Si hay terroristas que permanecen escondidos entre la población, a investigadores y sistemas informáticos les costará mucho encontrarlos. La mayoría de los sistemas de extracción de datos y de fusión tienen algún tipo de ajuste de sensibilidad: si se la disminuye, el sistema no encuentra nada; si se la aumenta, el sistema saca demasiadas conclusiones que resultan equivocadas. ¿Cómo ajustarla entonces? Si el sistema señala a uno de cada tres pasajeros de avión como una amenaza potencial, tendrá muchas probabilidades de detectar a los terroristas. Pero también paralizará el tráfico aéreo y hará imposible la aplicación de las leyes.

Si un sistema de fusión de datos no funciona como es debido, quizá se debe a que los algoritmos están mal diseñados. Pero el problema podría también ser la escasez de datos. Del mismo modo, si el sistema está aportando buenos resultados, suministrarle un mayor número de datos puede aumentar su eficiencia. En otras palabras, no importa cuán eficaz sea un sistema, hay una tendencia natural por parte de los creadores y usuarios de estos sistemas a querer más y más datos de entrada. Una tendencia natural así conduce a los proyectos de fusión de datos a la saturación, con la consiguiente preocupación no sólo de los defensores de las libertades civiles, sino también de los que pagan la factura. En su artículo de 1994, Clarke llegó a la conclusión de que "cuando choca el interés del Estado por controlar a la sociedad y el interés individual de los ciudadanos por la libertad, siempre sale ganador el Estado".

Lo frustrante del debate público sobre la fusión de datos para un científico como yo es que se haya dado a conocer a los ciudadanos tan poca información acerca de los sistemas de fusión que se están usando realmente. Este secretismo recuerda a los debates sobre la criptografía de los años noventa, cuando el gobierno de EE.UU. afirmaba que hay muchas razones para limitar por ley el uso de la criptografía, y al mismo tiempo defendía que dichas razones eran tan delicadas, que discutirlas en público constituiría una amenaza para la seguridad nacional. Sospecho que está surgiendo un debate similar sobre el uso por parte del gobierno de la fusión de datos, sin mencionar las posibles aplicaciones de esta poderosa técnica en el mundo de los negocios e incluso en política. Se trata de un debate que merece la pena mantener, y mantenerlo en público.

Bibliografía complementaria

COMPUTER MATCHING BY GOVERNMENT AGENCIES: THE FAILURE OF COST/BENEFIT ANALYSIS AS A CONTROL MECHANISM. Roger Clarke en *Information Infrastructure & Policy*, vol. 4, n.º 1, págs. 29-65; marzo 1995.

DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY. Simson Garfinkel. O'Reilly, 2000.

FORENSIC FEATURE EXTRACTION AND CROSS-DRIVE ANALYSIS. Simson L. Garfinkel en *Digital Investigation*, vol. 3, suplemento 1, págs. 71-81; septiembre 2006.

THREAT AND FRAUD INTELLIGENCE, LAS VEGAS STYLE. Jeff Jonas en *IEEE Security & Privacy*, vol. 4, n.º 6, págs. 28-34; noviembre/diciembre 2006.



LA CRIPTOGRAFIA MODERNA puede proteger la información privada aun cuando haga uso de ella colectivamente.

PROTECCION DE SECRETOS

Diversas técnicas informáticas protegen la privacidad de la información y de las actividades en la Red hasta el punto y con el detalle que se desee

Anna Lysyanskaya

Quim ha decidido probar la agencia de contactos en línea SíySí.com. En el sitio Web abre una cuenta y rellena varios formularios, donde detalla sus datos personales y qué busca en una potencial compañera. Casi instantáneamente, el servicio le presenta un grupo de posibles almas gemelas, entre cuyos nombres aparece uno que le llama la atención, Cum. Quim le envía su dirección electrónica acompañada del que, cree, es un simpático mensaje inaugural. Ella le contesta inmediatamente y comienza un arrollador romance electrónico.

Pobre Quim. Poco ha tardado en recibir también un aluvión de llamadas telefónicas no deseadas de grupos de activistas y de unos vendedores que parecen saber muchas cosas de él; su seguro médico privado le inquiere acerca de sus arriesgadas vacaciones. ¿Qué ha sucedido? Los dueños de SíySí, carentes de escrúpulos, han ido vendiendo información sobre sus clientes. Y luego está Kam, un compañero de trabajo guasón a quien Quim, estúpidamente, ha mostrado uno de los mensajes electrónicos de Cum. Quim ignora que varios de los últimos mensajes de Cum son una impostura de Kam.

Alicia, en cambio, vive en la gloria, como su nuevo amigo Juan. Los dos se han conocido a través de SophisitiCats.com, una agencia matrimonial que ofrece lo último en herramientas criptográficas. Alicia accede a su sitio Web protegida por una autorización anónima, un sistema que garantiza que nadie de la agencia podrá rastrear quién es ni cuándo accede al sitio. SophistiCats emplea un programa que proporciona "evaluación segura de funciones" para contrastar sus características personales y preferencias con los de Juan, por lo que nadie de la agencia conoce esa información y ni siquiera su emparejamiento con Juan: ¡La agencia de contactos no sabría casi nada de sus clientes!

Alicia contactó con Juan por medio de un "canal anónimo", y él contestó por la misma vía; ni siquiera su proveedor de Internet (ISP) sabe que es con Juan con quien contacta, ni lo que dicen los mensajes, y el ISP de Juan no está mejor informado sobre ella. Aunque Eva, la compañera de cuarto de Alicia, *sí* lo sabe, pero sólo porque Alicia le ha hablado de Juan y ha pegado copias de algunos mensajes en su ordenador. Eva podría suponer un problema, porque es una bromista redomada capaz de fisgonear en los mensajes que entran y salen del ordenador de Alicia y de alterarlos (es ella quien controla la red que conecta las dos a Internet). No hay peligro: el cifrado garantiza que Eva de nada puede enterarse fuera de lo que Alicia le ha mostrado, y las "firmas digitales" en los correos electrónicos de Alicia y Juan hace que para ellos sea pan comido localizar e ignorar los mensajes fingidos de Eva.

Cifrado total

Como Alicia y Quim, muchos realizamos electrónicamente un gran número de nuestras transacciones personales, económicas y oficiales. Tantas cosas podemos hacer con un ordenador conectado a Internet —de mante-

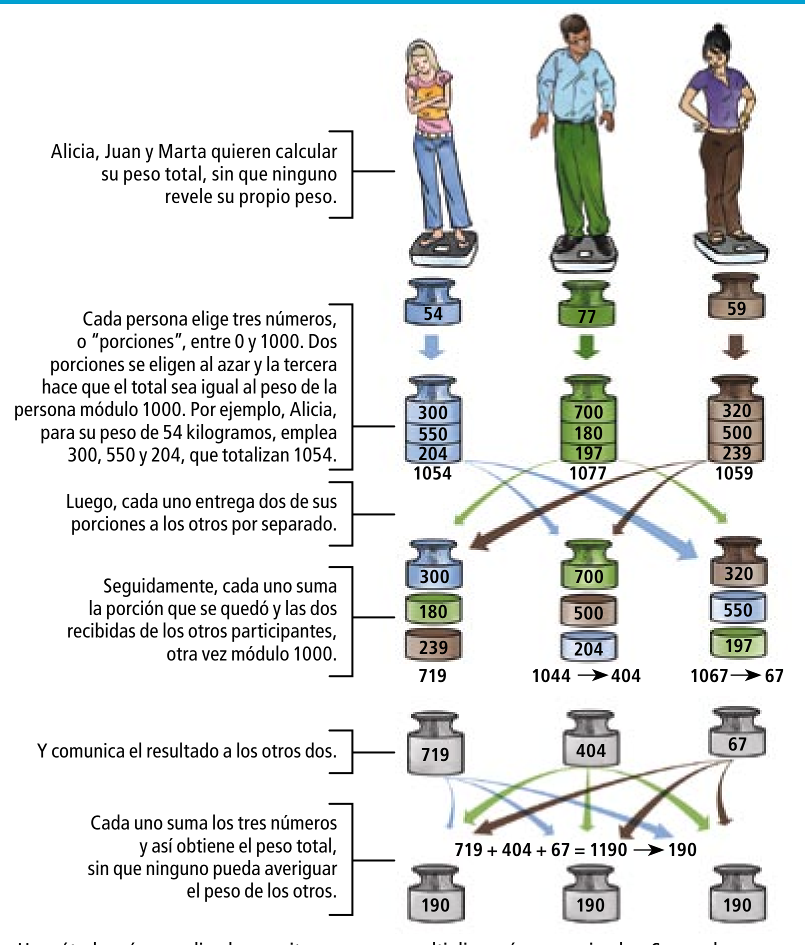
CONCEPTOS BASICOS

- La variedad de herramientas matemáticas que la criptografía moderna ofrece para proteger la privacidad y la seguridad rebasan largamente las posibilidades de la criptografía clásica.
- Es posible impedir que otros se enteren furtivamente de lo que decimos y a quién se lo decimos.
- Se puede preservar el anonimato incluso en actividades en línea que requieren registrarse y probar algo acerca de la propia persona.
- Un grupo puede calcular prácticamente cualquier cosa a partir de los datos colectivos de sus miembros (por ejemplo, quién es el ganador en una votación entre todos), sin que nadie revele dato personal alguno.

KENN BROWN *Mondolithic Studios*

Cálculos en compañía

La evaluación segura de funciones permite que un grupo de personas calcule cualquier cosa a partir de datos privados de cada uno, sin que nadie revele sus propios datos en el proceso.



Un método más complicado permite a un grupo multiplicar números privados. Sumando y multiplicando bits, podría calcular todo lo que pueda evaluar un ordenador a partir de sus datos privados. El sistema completo protege también contra quienes se apartan de las reglas.

nernos en contacto con nuestras amistades a comprar y vender todo género de artículos— que informarse con pelos y señales acerca de cualquiera es tan sencillo como registrar sus actividades en Internet. Y por varias razones, los ISP ya están registrando actividades nuestras; por ejemplo, los sitios Web que hemos visitado y cuándo. No sólo ellos. Muchas de las entidades con las que interactuamos en línea —comercios, periódicos, agencias de contactos— también nos mantienen muy vigilados. Por tanto, si valoramos la intimidad, nos enfrentamos al problema de aprovechar lo que Internet ofrece sin renunciar a ella.

Un asombroso descubrimiento de la criptografía moderna es que casi cualquier tarea en la que intervenga la comunicación electrónica puede efectuarse reservadamente. Muchos, incluidos los autores de bastantes diccionarios, creen equivocadamente que criptografía es sinónimo de estudio del cifrado. Pero la criptografía moderna abarca mucho más. Así, ofrece métodos matemáticos para proteger las comunicaciones y la informática de toda clase de conductas malintencionadas; es decir, herramientas para proteger nuestra intimidad y seguridad.

Supongamos, por ejemplo, que los miembros de un grupo conectado por Internet desean calcular algo que depende de datos procedentes de cada uno de ellos, datos que desean mantener en privado. Los datos podrían ser el voto en unas elecciones; querrían saber el resultado sin revelar el voto de cada uno. Un procedimiento conocido como cálculo multiparte o evaluación segura de funciones (SFE) les permite contar los votos de tal modo, que cada participante sepa el resultado sin enterarse del voto de nadie más; ni siquiera una coalición de miembros malévolos del grupo, que interceptaran mensajes en la red y pusiesen en su lugar mensajes amañados. El protocolo SFE puede también proporcionar a cada individuo un resultado en privado, tal como hace nuestra agencia SophistiCat.

En la SFE, los datos de cada participante se dividen en porciones que se distribuyen entre el resto del grupo. Seguidamente, cada participante opera sobre las porciones bajo su control (sumándolas, redistribuyendo porciones del resultado, etcétera). Al final, el grupo vuelve a juntar las piezas para obtener el resultado definitivo. Nadie, en ningún momento, dispone de la información necesaria para reconstruir los datos de otra persona.

Quizá no sorprenda que una función tan sencilla como sumar votos pueda evaluarse con seguridad, pero recordemos lo que SophistiCat hizo por Alicia: averiguó qué miembros entre sus miles de clientes eran buenos partidos para ella; sobre ellos le ofreció una información limitada, y todo sin que el mismo sistema se enterara de ningún dato de ella ni de nadie más. Una organización Gran Hermano que interceptara furtivamente el tráfico de la Red o rebuscara en la información contenida en los discos duros de SophistiCat sería igualmente incapaz de enterarse de nada.

SophistiCat es una agencia imaginaria, pero los criptógrafos han mostrado cómo podría hacerse realidad. En enero pasado se empleó SFE para un problema del mundo real (en Dinamarca, al menos): fijar el precio de los contratos de remolacha azucarera de unos 1200 agricultores daneses, tomando como base las ofertas que cada uno de ellos hacía en privado. Con SFE tenemos todas las ventajas de nuestra parte: la funcionalidad que deseamos de Internet sin sacrificar la privacidad.

Aunque la capacidad del protocolo SFE es muy grande, su potencia e inespecificidad

FECHAS CLAVE

Alrededor de 800 a.C.: Al-Kindi, erudito y matemático árabe que vive en Bagdad, escribe *Sobre el descifrado de mensajes criptográficos*, con la primera exposición conocida del análisis de frecuencias y otras técnicas criptoanalíticas.

1586: Thomas Phelippes emplea el análisis de frecuencias para descifrar mensajes entre María I de Escocia y los conspiradores contra la reina Isabel I de Inglaterra. María y los conspiradores fueron ejecutados.

MATT COLLINS

tiene un precio: consume grandes dosis de cálculo y comunicación. Aunque es suficiente para ciertas tareas, unas elecciones por ejemplo, todavía resulta demasiado engorroso para ponerlo en funcionamiento cada vez que activamos un vínculo con una página Web segura. Los expertos en informática han desarrollado protocolos especializados mucho más eficaces que SFE para tareas comunes concretas. Entre ellos están:

Cifrado. Ni el ISP de Alicia ni el de Eva pueden descifrar los mensajes que Alicia envía a Juan. El tráfico entre el ordenador de Alicia y SophistiCat también es seguro.

Autenticación. Alicia puede estar segura de que los mensajes proceden de Juan, no de Eva.

Canales anónimos. El ISP de Alicia no sabe a quién manda ella sus mensajes ni si ha visitado alguna vez el sitio Web de SophistiCats.

Prueba de conocimiento cero. Alicia puede probar a otra persona que algo es verdad sin revelar la prueba.

Autorización anónima. SophistiCats sabe que Alicia es uno de sus miembros cuando accede al sitio Web, pero ignora quién es. Este protocolo es un caso particular de prueba de conocimiento cero.

Mensajes secretos

El más antiguo de los problemas básicos que estudia la criptografía, y uno de los más fundamentales, es el del cifrado: cómo comunicarse con seguridad por un canal no seguro (un canal que un adversario puede intervenir furtivamente). Alicia quiere enviar un mensaje a Juan, pero Eva controla parte del canal (a través de la red del apartamento) que Alicia va a utilizar. Alicia quiere que Juan, y no Eva, lea el mensaje.

Al analizar este problema, adviértase, primero, que Juan debe saber algo que Eva no sabe; si no, Eva podría hacer exactamente lo mismo que Juan. Lo que sólo Juan sabe es su propia clave secreta (SK). Segundo, adviértase que Alicia debe saber algo sobre la SK de Juan, de modo que le sea posible crear un criptograma —un mensaje cifrado— específicamente para Juan. Si Alicia conoce la SK misma, el protocolo se llama cifrado de clave secreta, el tipo de cifrado que se conoce y practica desde hace siglos.

En 1976 Whitfield Diffie y Martin E. Hellman, por entonces ambos en la Universidad de Stanford, concibieron otra posibilidad, el cifrado de clave pública, para la cual Alicia no necesita saber la SK. No necesita más que un valor público emparentado con la SK, que llamamos clave pública (PK) de Juan. Alicia emplea la PK de Juan para cifrar su mensaje, y sólo Juan, con su SK, puede descifrar el criptograma resultante. No importa que Eva conozca también la PK de Juan porque ella no puede usarla para descifrar el criptograma. Diffie y Hellman propusieron la idea de la clave pública, pero sin saber aún cómo ponerla en práctica. Ello vino un año después, cuando Ronald L. Rivest, Adi Shamir y Leonard M. Adleman, los tres por entonces en el Instituto de Tecnología de Massachusetts, presentaron la primera elaboración de un criptosistema en clave pública: el algoritmo RSA.

El funcionamiento del algoritmo para el cifrado de clave pública se basa en una función con "trampilla". Esa función es fácil de calcular para generar el criptograma y difícil de invertir para recuperar el texto sin cifrar, salvo que se haga uso de una trampilla especial. La trampilla sirve de clave secreta. El algoritmo RSA fue el primer ejemplo de función con trampilla. Sus autores ganaron el premio A. M. Turing de 2002, el más prestigioso de la ciencia de la computación.

El hallazgo del RSA, aclamado como un gran avance de los fundamentos de la criptografía, alimentó años de posteriores investigaciones sobre el cifrado y, más en general, sobre la criptografía. Sobre el cifrado aún queda mucho

FECHAS CLAVE

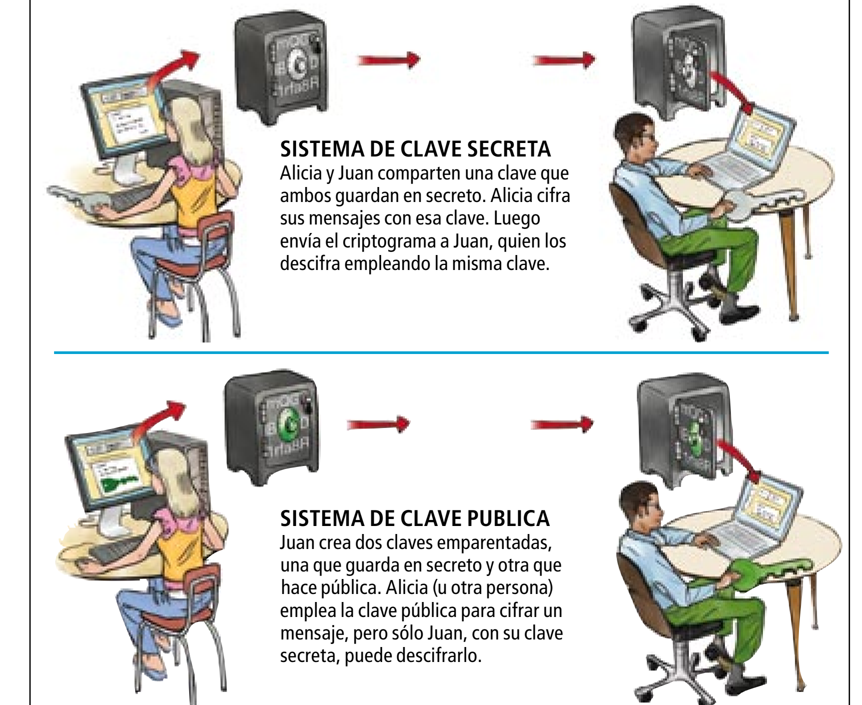
1918: El comandante Joseph O. Mauborgne, del ejército de EE.UU., y Gilbert Vernam, de los Laboratorios AT & T Bell, inventan el código de un solo uso, cuya clave aleatoria secreta es tan larga como el mismo mensaje y se emplea una única vez.

1944: En Bletchey Park (Inglaterra), Colossus (la primera calculadora programable de válvulas de vacío) descifra los mensajes cifrados del Alto Mando alemán. Facilitó valiosa información antes del día D del desembarco en Normandía.

1945: Claude Shannon, de los Laboratorios AT & T Bell, demuestra que el código de un solo uso es inviolable incluso ante un adversario provisto de una potencia de cálculo ilimitada. Esta definición de secreto es tan fuerte, empero, que Shannon prueba además que el código de un solo uso es el único criptosistema que la cumple.

Ocultación de contenidos

Las técnicas modernas de codificación de información son de dos tipos: cifrado de clave secreta y cifrado de clave pública.



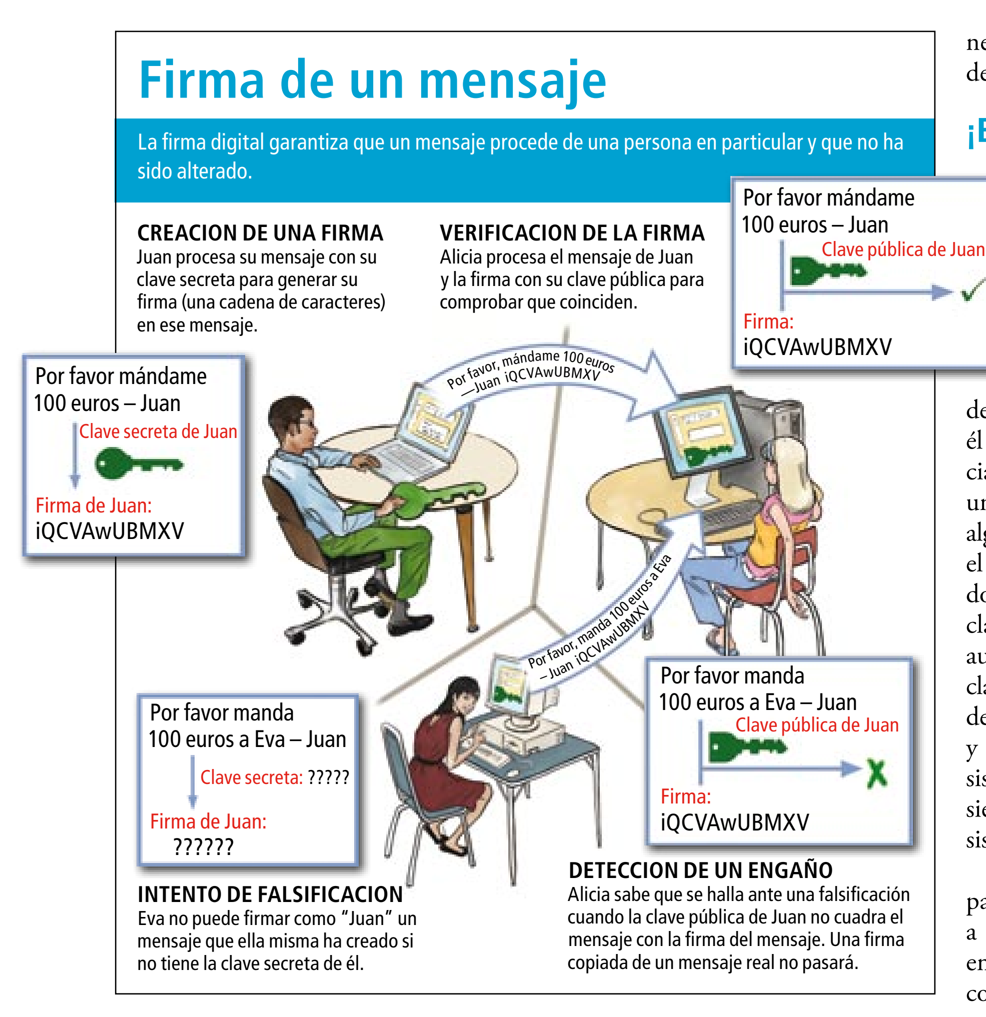
SISTEMA DE CLAVE SECRETA
Alicia y Juan comparten una clave que ambos guardan en secreto. Alicia cifra sus mensajes con esa clave. Luego envía el criptograma a Juan, quien los descifra empleando la misma clave.

SISTEMA DE CLAVE PUBLICA
Juan crea dos claves emparentadas, una que guarda en secreto y otra que hace pública. Alicia (u otra persona) emplea la clave pública para cifrar un mensaje, pero sólo Juan, con su clave secreta, puede descifrarlo.

MATT COLLINS

Firma de un mensaje

La firma digital garantiza que un mensaje procede de una persona en particular y que no ha sido alterado.



CREACION DE UNA FIRMA
Juan procesa su mensaje con su clave secreta para generar su firma (una cadena de caracteres) en ese mensaje.

VERIFICACION DE LA FIRMA
Alicia procesa el mensaje de Juan y la firma con su clave pública para comprobar que coinciden.

INTENTO DE FALSIFICACION
Eva no puede firmar como "Juan" un mensaje que ella misma ha creado si no tiene la clave secreta de él.

DETECCION DE UN ENGAÑO
Alicia sabe que se halla ante una falsificación cuando la clave pública de Juan no cuadra el mensaje con la firma del mensaje. Una firma copiada de un mensaje real no pasará.

FECHAS CLAVE

1976: Whitfield Diffie y Martin E. Hellman, ambos de la Universidad de Stanford, proponen el cifrado de clave pública y la autenticación.

1977: Ronald R. Rivest, Adi Shamir y Leonard M. Adleman, los tres en el Instituto de Tecnología de Massachusetts, elaboran el primer criptosistema de clave pública, el algoritmo RSA.

Octubre 1977: En la sección de Martin Gardner de *Investigación y Ciencia*, Rivest y otros desafían a los lectores a descifrar un mensaje codificado mediante el algoritmo RSA con una clave de 129 dígitos (RSA-129). Calculan que podrían pasar 40.000 billones de años antes de que alguien lo lograse.

y difícil por hacer, desde descubrir nuevas funciones con trampilla, hasta estudiar las hipótesis matemáticas en las que se basa la seguridad de una función específica o definir exactamente los requisitos que debe cumplir un sistema de cifrado para que se le considere seguro.

El cifrado de clave pública posibilita las compras en línea sin enviar abiertamente por Internet información sensible, como el número de una tarjeta de crédito. El navegador del comprador hace el papel de Alicia, el sitio Web, el de Juan. Por lo general, el https, un protocolo que hoy es compatible con la mayoría de los navegadores, hace uso de cifrado de clave pública para facilitar la navegación por un canal cifrado (búsquese "https://" en el URL [la dirección del sitio Web] y un icono que representa un candado cerrado en la barra de estado del navegador).

Muchos emplean también cifrado de clave pública para proteger el correo electrónico. Para ello hay programas en abundancia, incluido el paquete GNU Privacy Guard (disponible en www.gnup.org), que la Free Software Foundation presentó hace diez años. Un correo electrónico no codificado viaja por Internet en una forma que es fácil de leer y podría permanecer así en distintos discos duros a lo largo del trayecto hasta pasado algún tiempo.

¡Eh, soy yo!

Estrechamente vinculado al problema del cifrado está el de la autenticación. Supongamos que Alicia recibe el mensaje "Alicia, manda 100 euros a Eva. Besos, Juan." ¿Cómo sabe ella que procede realmente de su novio y que no es una impostura de Eva?

Igual que en el caso del cifrado, Juan debe saber algo que Eva no sepa, de modo que él pueda, y Eva no, generar un mensaje que Alicia aceptará. Por tanto, Juan vuelve a necesitar una clave secreta. Además, Alicia necesita saber algo sobre la SK de Juan para poder verificar que el mensaje procede de él. Una vez más, existen dos variedades de protocolo: autenticación por clave secreta, más conocida como código de autenticación de mensajes, y autenticación por clave pública, muchas veces citada como sistema de firma digital, o de firma electrónica. Diffie y Hellman fueron los primeros en prever los sistemas de firma digital, a la vez que propusieron el cifrado de clave pública. El primer sistema se basó en el algoritmo RSA.

La idea rectora es que Juan emplea su SK para calcular una "firma" que agrega ("anexa") a su mensaje y que Alicia, u otra persona, emplea entonces su PK para verificar que casa con el mensaje en cuestión. Alicia sabe que el mensaje es de Juan porque nadie más tiene la SK necesaria para generar la firma válida.

Actualmente es fácil engañar a un usuario de correo electrónico para que crea que un mensaje es de Juan cuando en realidad es de Eva. Un correo electrónico imitado puede incluir noticias falsas y cotizaciones de bolsa incorrectas. Pero si se autenticaran todas las comunicaciones de correo electrónico, tales ataques serían imposibles: el usuario de correo electrónico pondría su firma digital en todos los mensajes emitidos y verificaría las firmas digitales de todos los recibidos. La autenticación podría también combatir el correo no deseado haciendo que los servidores rechacen el correo entrante no autenticado por el remitente. Cuando se creó el correo electrónico, en los años setenta, no existían protocolos de autenticación y aún rigen muchas convenciones de aquellos años.

Hay programas gratis de firma y autenticación de firmas digitales; por ejemplo, como parte del paquete GNU Privacy Guard ya mencionado antes.

Cebollas

Codificando nuestros mensajes, podemos evitar que el ISP (o cualquier otro curioso subrep-

MATT COLLINS

ticio) descubra qué enviamos y qué recibimos, pero no con quién nos comunicamos. Por ejemplo, el ISP de Alicia sabrá si ella entra en un sitio Web de Alcohólicos Anónimos. Imaginemos que el ISP vendiese esa información a una compañía de seguros de automóviles. La gente se vería menos inclinada a buscar la ayuda en línea porque les inquietaría que ello aumentara la prima de su seguro.

El problema puede solventarse con la SFE: lo que Alicia introduciría de modo privado sería el URL al que ella quiere ir, y lo que en privado obtendría sería el contenido de la correspondiente página Web. Emplear SFE, empero, sería muy ineficaz. En 1981 David Chaum, por entonces en la Universidad de California en Berkeley, propuso una solución mucho más sencilla: los canales anónimos, hoy conocida también como encaminamiento cebolla.

Tal como sugiere el nombre, Alicia manda su mensaje envuelto en capas. Cifra cada una de ellas (y todo lo que encierra) valiéndose de la clave pública de una persona diferente y luego añade la dirección de esa persona al exterior de la capa. Un mensaje de Alicia para Juan podría seguir el trayecto siguiente: Alicia le manda la cebolla a Marcos, que retira el catafilo más externo, descifrando la cebolla con su clave secreta. Dentro, Marcos encuentra una cebolla más pequeña y la dirección de Lisa, quien la descifra con su clave, y así sucesivamente. Finalmente, Juan recibe el corazón de la cebolla y lo descifra para hacerse con el mensaje de Alicia.

En la práctica, los intermediarios son partes de una red de ordenadores montada especialmente para proceder al descifrado y reenvío de modo automático. Idealmente, cada intermediario recibe sin cesar una gran cantidad de cebollas y las reemite en orden aleatorio. Aun cuando un ISP estuviera observando sin parar a todos los intermediarios, no podría saber a dónde fue el mensaje de Alicia, ni de dónde venía el mensaje de Juan, siempre que en la red haya un tráfico de cebollas suficiente.

Ni siquiera Juan sabrá quién le envió el mensaje, a menos que Alicia decida revelar su identidad en él. Pero, pese a que ella mantenga el anonimato, él aún podrá mandarle a Alicia una respuesta anónima si ella hubiese incluido una "cebolla respuesta" que contuviese las capas de direcciones y claves públicas necesarias para encaminar un mensaje de vuelta.

Seguiría siendo imposible rastrear los mensajes de Alicia y Juan, incluso en el caso de que algún intermediario filtrase información

FECHAS CLAVE

1982: Shafi Goldwasser y Silvio Micali, por entonces doctorandos de la Universidad de California en Berkeley, desarrollan los fundamentos definitorios de la criptografía moderna, incluida una definición práctica de seguridad.

1985: Goldwasser, Micali y Charles Rackoff, de la Universidad de Toronto, idean las pruebas de conocimiento cero. Un año después, Oded Goldreich, del Technion-Instituto de Tecnología de Israel en Haifa, Avi Wigderson, de la Universidad Hebrea de Jerusalén, y Micali crean la prueba de conocimiento cero para la tricoloración de dibujos.

1987: Goldreich, Wigderson y Micali elaboran los protocolos para el cálculo multiparte, o evaluación segura de funciones, basándose en un protocolo biparte creado por Andrew C. Yao, de la Universidad de Princeton.

Ocultación de conexiones

Puede enviarse información anónimamente mediante protocolos tales como el encaminamiento cebolla, en el que los datos y también la ruta a seguir están encerrados bajo múltiples capas de codificación.

ENVIO DE UNA CEBOLLA

Alicia cifra primero el mensaje con una serie de claves públicas pertenecientes a intermediarios elegidos aleatoriamente, y así resulta una cebolla de muchas capas cifradas. En las capas introduce asimismo las instrucciones de encaminamiento.



Le envía la cebolla a Marcos, cuya clave secreta descifra la capa más exterior de la codificación. "Dentro" halla una cebolla con la dirección de Lisa, a quien remite la cebolla.

La clave secreta de Lisa elimina la capa siguiente de la cebolla, y dentro encuentra otra cebolla con una dirección, a la cual envía la cebolla, y así sucesivamente.

Por último, Luis destapa el corazón de la cebolla y se lo manda a Juan, quien lo abre con su clave secreta para dar con el mensaje. Nadie salvo Alicia sabe la ruta seguida por la cebolla.

LA RED

La ruta que sigue la cebolla de Alicia (*violeta*) a través de la red de intermediarios queda oculta a la observación furtiva si hay suficiente información circulando por la red.

MATT COLLINS

Acreditación sin identificación

Haciendo uso de la autorización anónima, un suscriptor a un sitio Web podría inscribirse como usuario legítimo y registrado, sin dar ningún atisbo de su identidad. El sitio Web ni siquiera sería capaz de asociar el usuario a sus propias visitas anteriores. Ese protocolo constituye un ejemplo de prueba de conocimiento cero, en la que una parte demuestra un hecho sin revelar nada acerca de la prueba, salvo su validez.

Imaginemos a Alicia y Juan jugando con un dibujo, tres lápices de colores y unos vasos de papel. El dibujo está formado por un conjunto de puntos, o vértices, enlazados por líneas rectas. De dos vértices enlazados por una línea se dice que son contiguos. Sólo algunos dibujos son tricoloreables, con lo que quiere decirse que bastan tres colores para colorear todos los vértices sin que dos vértices contiguos tengan el mismo color. Alicia demostrará a Juan que ella ha tricoloreado su dibujo sin darle a él pista alguna acerca de cómo hacerlo.

El juego comienza con Juan fuera de la habitación. Alicia hace seis copias del dibujo. Dado que sabe cómo tricolorear el dibujo, tricolorea una de las copias. Con las otras cinco, utiliza las seis posibles permutaciones de los colores. Por tanto, las seis copias del dibujo están tricoloreadas de modos trivialmente diferentes. Elige una copia al azar, la pone sobre la mesa y tapa cada vértice con un vaso. Juan regresa y debe retirar los vasos de dos vértices contiguos cualesquiera que elija. Si los vértices tienen el mismo color, sabrá que Alicia ha mentido y que no ha hecho un tricoloreado válido.

Siguen iterando el procedimiento de inspección: Juan sale de la habitación en cada ocasión, mientras Alicia elige al azar una de las seis copias del dibujo para poner los vasos sobre ella. Desde la perspectiva de Juan, si Alicia hace trampas, podría estar mostrándole muchos tricoloreados inválidos, y la delatora coincidencia de color entre dos vértices contiguos no tendría por qué estar en el mismo lugar en cada uno. Pero conforme se suceden las comprobaciones, la probabilidad de que sorprenda el engaño se acercará al 100 por ciento. Sin embargo, cuando todo termine, él no sabrá cómo Alicia coloreó el dibujo. En cada comprobación, los colores que él ve en los vértices elegidos son aleatorios; los habría podido elegir incluso él mismo.



Para cualquier declaración que requiera una prueba relativamente corta (tal como "Tengo las credenciales que me identifican como usuario autorizado y mayor de 18 años"), es posible elaborar una versión de este juego que confirme la declaración sin revelar ninguna información adicional (tal como "Soy Alicia" o "Soy el usuario n.º 4790561").

MATT COLLINS

FECHAS CLAVE

1994: Netscape Communications lanza el protocolo Secure Sockets Layer, que emplea cifrado de clave pública para la seguridad de las transacciones en la Red.

1994: Arjen K. Lenstra, de Bell Communications Research, y más de 600 voluntarios de Internet, con más de 1600 ordenadores que ejecutaban a la vez algoritmos de factorización recientes, tardaron ocho meses en factorizar el RSA-129. Revelaron así el mensaje de la apuesta de 1977: "LAS PALABRAS MAGICAS SON: ESCRUPULOSO QUEBRANTAHUESOS".

2008: Un PC actual tardaría más de mil billones de años en descerrajar una clave RSA de la longitud recomendada (2048 bits).

acerca de lo que estaban haciendo. Cuantos más participantes usasen ese sistema y prestasen voluntariamente sus ordenadores para servir como intermediarios, más difícil se iría haciendo adivinar quién estaba hablando con quién.

Al igual que para el cifrado y las firmas digitales, hay programas gratis para quienes deseen comunicarse a través de canales anónimos o participar como intermediarios. El proyecto Encaminador Cebolla (Onion Router), por ejemplo, puede encontrarse en www.torproject.org.

Accesos privados

Supongamos que Alicia está suscrita a la revista en línea SophistiCat American. Se conecta a la revista vía un canal anónimo, accede con su nombre de usuario y su contraseña, y procura que todos los mensajes, entrantes y salientes, estén cifrados. ¿Supone ello que puede estar segura de que nadie descubrirá lo que está haciendo en la línea? No, desde luego; la revista sabe exactamente lo que Alicia está haciendo.

Puede que Alicia intente borrar su rastro empleando un seudónimo al suscribirse, pero los hábitos de lectura de ese seudónimo podrían no tardar en señalar su identidad. Consultando la previsión meteorológica podría revelar su código postal, introducir la fecha de su nacimiento para ver su horóscopo y revelar su posible sexo leyendo sobre el cáncer de mama. Esas tres informaciones —código postal, fecha de nacimiento y sexo— bastan para identificar inequívocamente al 87 por ciento de los estadounidenses.

Sorpresa: el problema de Alicia tiene una solución criptográfica, la autorización anónima. Alicia puede probar a la revista que es una suscriptora cada vez que entra en la página Web. Sin embargo, esa prueba nada revela acerca de qué suscriptora es en concreto; ni siquiera, por ejemplo, que es la misma persona que accedió unas pocas horas antes. Este protocolo es un caso particular del más general protocolo de conocimiento cero.

Con una prueba de conocimiento cero, Alicia puede convencer a Juan de que una afirmación es cierta sin revelar por qué es cierta,

sin aportar la menor información adicional. Para demostrar la afirmación “Soy un usuario autorizado de SophistiCat American”, la revista en línea o un tercer servicio le enviaría a Alicia, cuando se suscribiese, una credencial propia, algo así como una clave secreta. Luego, cada vez que la revista lo pidiese, Alicia haría uso de esa clave para demostrar que su credencial es válida, sin revelar la credencial en sí. Con credenciales procedentes de autoridades diferentes Alicia podría aportar una prueba de conocimiento cero de afirmaciones más complicadas, tales como “Soy una usuaria autorizada de más de 18 años”.

La idea básica del funcionamiento de una prueba de conocimiento cero se ilustra con la situación descrita en el recuadro “Acreditación sin identificación”, en la que Alicia demuestra a Juan que tiene un diagrama coloreado de una cierta manera (técnicamente, que tiene “un grafo tricoloreado”), pero sin mostrarle a Juan de qué manera lo coloreó. Tricolorear un grafo es un problema de los llamados NP-completos [*véase* “Los límites de la computación cuántica”, por Scott Aaronson; INVESTIGACIÓN Y CIENCIA, mayo 2008]. Aquí, lo que importa de la “NP-completitud” es que se puede elegir cualquier afirmación para la que se disponga de una prueba razonablemente corta y elaborar una versión del juego de Alicia y Juan que dé una prueba de conocimiento cero de esa afirmación.

El protocolo de tricoloración pone de manifiesto los principios que posibilitan las pruebas de conocimiento cero, pero es poco eficaz en la práctica, a la manera en que es ineficaz la evaluación segura de funciones general. Afortunadamente, los criptógrafos han elaborado para tipos específicos de credenciales unos protocolos similares que servirían para la autorización anónima eficaz.

Descerrajar los códigos

¿Cuánta seguridad brinda la seguridad? Cuando Alicia codifica un mensaje para Juan, ¿le es muy difícil a Eva descifrarlo? ¿Y si Eva dispone de cierta información interna o de oportunidades que le permiten entrar en el sistema sin violentarlo? Podría, por ejemplo, saber ya algo acerca del mensaje cifrado; quizás el nombre de un café del barrio donde Alicia y Juan van a reunirse por primera vez. O si “Juan” es un servidor seguro de la Web, Eva podría enviarle un galimatías cuidadosamente preparado, en vez del criptograma y, de sus respuestas, deducir pistas sobre la clave secreta. Una definición generalmente aceptada de seguridad para cifrado de clave pública tiene en cuenta todos esos supuestos y exige que Eva no consiga ni la más mínima información utilizable. Entre otros, el paquete GNU Privacy Guard supera la prueba.

El análisis de la seguridad de un criptosistema es una disciplina muy desarrollada. Al contrario de lo que suele creerse, la criptografía no es un juego del ratón y el gato en el que se supone que un sistema es seguro simplemente porque nadie ha mostrado cómo violarlo. Numerosos componentes básicos de la criptografía se basan en problemas matemáticos bien estudiados. Los criptógrafos no pueden demostrar con una certeza absoluta que un criptosistema sea inviolable, pero sí que todo algoritmo que lo viole es solución de un problema fundamental que ha tenido estancados a los mejores matemáticos y científicos de la computación.

Algunos protocolos dependen sólo de la existencia de una función matemática de un tipo particular. Por ejemplo, los criptógrafos saben cómo elaborar un criptosistema de clave pública a partir de una función con trampilla cualquiera. Y, si alguien viola las funciones empleadas en el RSA, éstas pueden ser sustituidas por otras que aún resistan.

Sólo rara vez se supone que un esquema sea seguro sobre una base más *ad hoc*. Pero ello sólo ocurre después de que centenares de investigadores de primera fila de todo el mundo hayan estudiado el algoritmo durante varios años. Los criptógrafos sólo pueden permitirse llevar a cabo ese proceso con unos pocos componentes básicos críticos. Seguidamente demuestran la seguridad de sistemas mayores, en el supuesto de que los componentes básicos sean seguros.

Los protocolos criptográficos pueden aportar soluciones de una versatilidad sorprendente a problemas de privacidad que parecen imposibles (tales como el de la autorización anónima). Pero muchos de los problemas a los que nos enfrentamos no son de naturaleza criptográfica. Si Alicia se halla bajo vigilancia constante en el mundo físico, magro consuelo es que sus actividades en línea estén protegidas. Ya hay cámaras que vigilan los espacios públicos en nombre de la ley. Quizá, para proteger la intimidad, los constructores de edificios podrían administrar la información de las cámaras instaladas en sus propiedades y la SFE encargarse de manejarla para seguir la pista de unos sospechosos sin almacenar las actividades de las demás personas en una base de datos central.

En líneas más generales, cuando la privacidad o la intimidad está amenazada por un sistema como el de vigilancia pública, deberíamos preguntarnos qué problemas aborda el sistema y si podremos salvaguardar nuestra privacidad recurriendo a la criptografía para resolverlos.

La autora

Anna Lysyanskaya, docente en la Universidad Brown, disfruta de una beca de estudios de la Fundación Nacional para la Ciencia de Estados Unidos y otra beca de investigación Sloan. Se doctoró en el Instituto de Tecnología de Massachusetts bajo la dirección de Ronald R. Rivest, la “R” del cifrado RSA. Los modelos de firmas y los protocolos de autorización anónima de su tesis forman hoy parte de la norma del Trusted Computing Group. Si el lector se compró un ordenador hace menos de dos años, es probable que su microprocesador los incorpore.

Bibliografía complementaria

ZERO-KNOWLEDGE SUDOKU. Lance Fortnow. (Cómo demostrar que se tiene la solución a un sudoku sin enseñarla.) Disponible en http://weblog.fornow.com/2006/08/zero-knowledge-sudoku.html

INTRODUCTION TO MODERN CRYTOGRAPHY. Jonathan Katz y Yehuda Lindell. Chapman & Hall/CRC, 2007. Primer capítulo disponible en www.SK.imd.edu/~jkatz/imc.html

MULTIPARTY COMPUTATION GOES LIVE. Peter Bogetoft y otros, febrero 2008. Disponible en http://eprint.iacr.org/2008/068


EL
CAF

¿EL FIN DE LA PRIVACIDAD?

Millones de personas comparten detalles íntimos de su vida en las redes sociales de Internet. Se augura un reajuste de las fronteras entre lo público y lo privado

Daniel J. Solove

Aunque tiene nombre propio, la mayoría lo conoce por "el chico de la Guerra de las Galaxias". Decenas de millones de personas en todo el mundo saben quién es. Pero debe la celebridad a uno de los momentos más penosos de su vida.

En 2002, cuando tenía 15 años, el chico de la Guerra de las Galaxias se filmó a sí mismo blandiendo un bastón recoge-pelotas de golf como si fuera una espada de luz. Sin el concurso de los coreógrafos de la película, se movía torpemente y a trompicones.

El vídeo fue descubierto por alguno de los atormentadores del muchacho. Lo colgó en la Red. El éxito fue instantáneo; los forofos, multitud. En toda la blogosfera, la gente empezó a remedarle, burlándose de su rechonchez, torpeza y pazguatez.

Surgieron de repente varias versiones del vídeo, enriquecidas con efectos especiales. Ciertos "admiradores" se dedicaron a editarlo para que el bastón recoge-pelotas fulgurase como una espada de luz. Le añadieron la música de *La Guerra de las Galaxias*. Otros lo mezclaron con otros vídeos. Se crearon docenas de versiones más o menos ornamentadas. El chico de la Guerra de las Galaxias apareció en un videojuego y en las series de televisión *Padre de familia* y *South Park*.

Una cosa es que tus compañeros de clase se burlen de ti y otra bien distinta, ser ridiculizado por el ancho mundo. El muchacho abandonó los estudios y tuvo que buscar ayuda psicológica. Lo que le ocurrió al chico de la Guerra de las Galaxias le puede ocurrir a cualquiera, y en un instante. Coleccionar información personal se ha convertido en algo normal. Cada día más personas adquieren teléfonos celulares, audiograbadoras digitales, cámaras Web y otros aparatos registradores que captan los detalles de la propia vida.

Por primera vez en la historia, casi todo el mundo puede difundir información a todos los puntos del globo. No hace falta una mínima fama para ser entrevistado por los medios de comunicación. Con Internet, cualquiera puede hacerse con una audiencia planetaria.

La técnica nos ha abocado a una división generacional. A un lado, los estudiantes de instituto y universitarios, cuya vida gira en torno a los blogs y redes sociales. Al otro lado, sus padres, para quienes la memoria del pasado suele permanecer trabada a unos recuerdos que se desvanecen o, en el mejor de los casos, a libros, fotografías y vídeos. Para la generación actual, el pasado se conserva en Internet, potencialmente para siempre. ¿Cuánta privacidad esperamos —y deseamos— en esta era de ubicua interconectabilidad?

Generación Google

La cantidad de jóvenes que acuden a las redes sociales (Facebook y MySpace) es pasmosa. En la mayoría de los campus universitarios estadounidenses, más del 90 por ciento de los estudiantes mantienen su propio sitio en la Red. Yo los llamo "generación Google". Para ellos, muchos fragmentos de información per-

CONCEPTOS BASICOS

- Las redes sociales facilitan la distribución a escala planetaria de chismorreos; las personas se han convertido en blanco de rumores compartidos por millones de usuarios de Internet.
- La exposición pública de las vidas privadas obliga a replantear nuestra concepción de la privacidad.
- Debe ampliarse la legislación para que contemple cierta protección de la privacidad, en cuanto a cosas que la gente dice y hace en lo que antes se habría considerado el dominio público.

HARRY CAMPBELL

DATOS Y CIFRAS

Más de **65.000** vídeos se reciben a diario en YouTube.

MySpace rebasó los **100 millones** de perfiles en 2006.

Desde 1999 el número de blogs ha crecido desde **50** a **50 millones**.

Más del **50 por ciento** de los blogs los escriben adolescentes de menos de **19** años.

sonal permanecerán para siempre en Internet, accesibles a ésta y a las generaciones futuras mediante una sencilla búsqueda en Google.

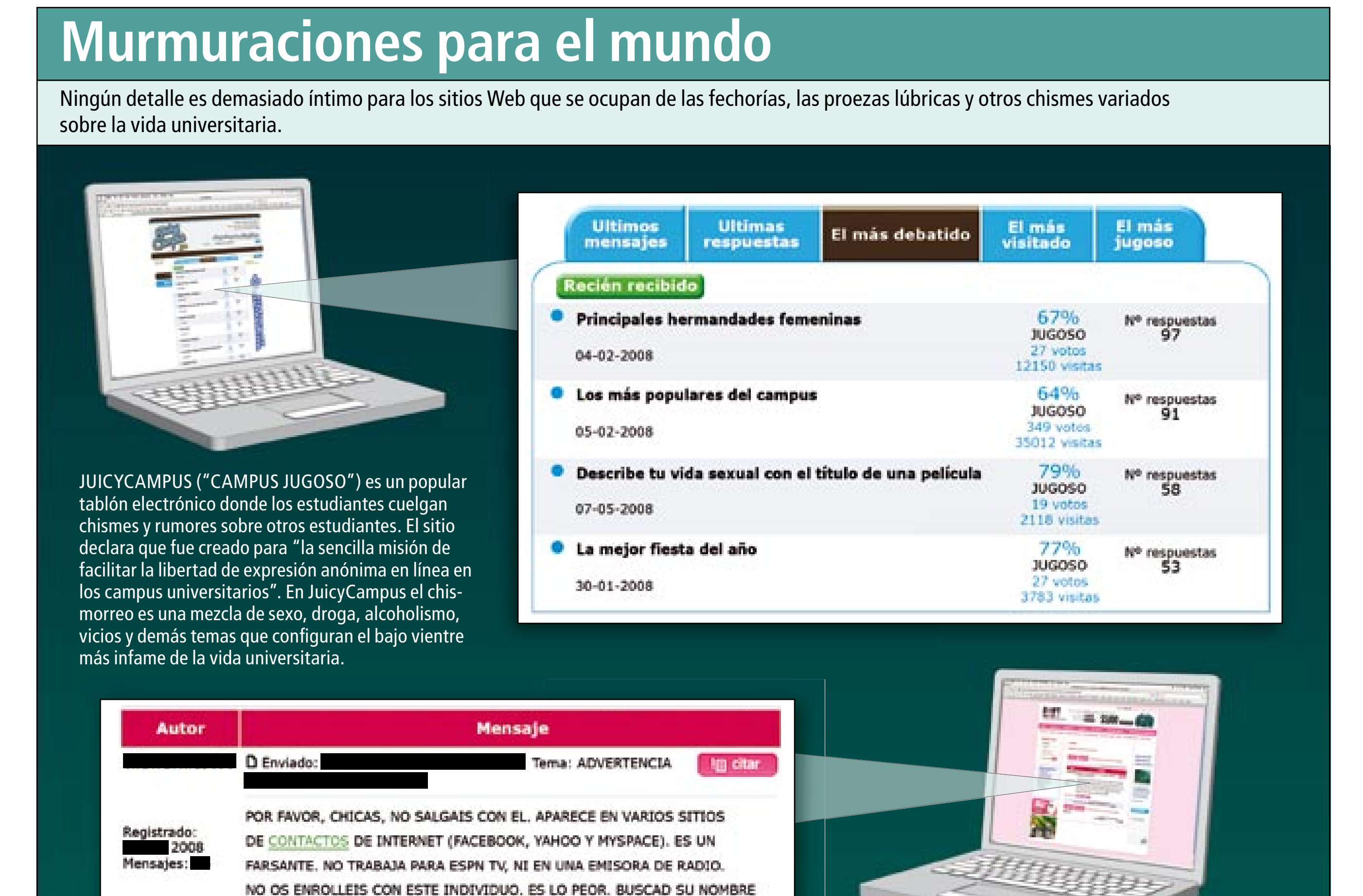
Tal transparencia es buena y mala a la vez. Ahora, las personas pueden divulgar sus ideas sin depender de editores, emisoras de radio, televisión u otros guardianes. Pero ese cambio genera también profundas amenazas a la privacidad y a la reputación. No es probable que al *New York Times* le interese el último chismorreo que circula en el instituto de Dubuque o en la Universidad estatal de Oregón. Pero sí puede preocuparles, y mucho, a los blogeros y demás comunicadores en línea. Para ellos, las anécdotas y rumores sobre amigos, enemigos, familiares, jefes, compañeros de trabajo y otras personas son pasto de primera para colgar en Internet.

Antes de Internet, los chismes corrían de boca en boca y no traspasaban los límites de un circulo social. Los detalles privados o íntimos estaban confinados en los diarios personales y encerrados en un cajón de escritorio. La interconexión social favorecida por Internet ha hecho que las comunidades de todo el planeta retornen a la cultura de la red social densa (*close-knit*), propia de la sociedad preindustrial, cuando casi todos los miembros de una tribu o de una aldea agrícola lo sabían todo sobre sus vecinos. Salvo que ahora los "aldeanos" pueblan el planeta entero.

Los estudiantes universitarios han empezado a compartir detalles obscenos acerca de sus compañeros. El sitio Web JuicyCampus opera a modo de tablón electrónico que permite a todos los estudiantes del país colgar, de forma anónima y sin comprobación, un sórdido despliegue de chismes sobre sexo, drogas y embriaguez. Otro sitio, Don't Date Him Girl ("Chica, no salgas con él"), invita a las mujeres a colgar quejas sobre los hombres con los que se hayan citado, junto con nombres y fotos auténticos.

Murmuraciones para el mundo

Ningún detalle es demasiado íntimo para los sitios Web que se ocupan de las fechorías, las proezas lúbricas y otros chismes variados sobre la vida universitaria.



JUICYCAMPUS ("CAMPUS JUGOSO") es un popular tablón electrónico donde los estudiantes cuelgan chismes y rumores sobre otros estudiantes. El sitio declara que fue creado para "la sencilla misión de facilitar la libertad de expresión anónima en línea en los campus universitarios". En JuicyCampus el chismorreo es una mezcla de sexo, droga, alcoholismo, vicios y demás temas que configuran el bajo vientre más infame de la vida universitaria.

DON'T DATE HIM GIRL ("CHICA, NO SALGAS CON EL") es un sitio Web que permite a las mujeres expresar sus opiniones acerca de los hombres con los que han salido. Sus relatos sobre tan díscolos individuos incluyen a menudo nombres verdaderos y fotografías. Quejas no verificadas proclaman a veces que esos hombres han transmitido enfermedades sexuales o que son maltratadores.

TOMMY MOORMAN; FUENTES: JUICYCAMPUS Y DON'T DATE HIM GIRL (*captura de pantalla*)

Las redes sociales y los blogs no constituyen la única amenaza. Tal como dejan patente varios artículos de este número, las empresas recogen y usan nuestra información personal a cada paso. El banco cuenta con un registro de las compras que realizamos con tarjeta de crédito. Si compramos en línea, los comerciantes guardan la etiqueta de cada artículo adquirido. Nuestro proveedor de Internet posee información acerca de cómo navegamos en la Telaraña. La compañía de televisión por cable tiene información sobre los programas que vemos.

Asimismo, el gobierno estadounidense compromete la privacidad organizando enormes bases de datos que pueden consultarse a la busca de patrones de conducta sospechosos. La Agencia Nacional de Seguridad escucha y examina las grabaciones de millones de conversaciones telefónicas. Otras agencias analizan las transacciones financieras. Miles de organismos federales y estatales poseen archivos de información personal, con el registro de nacimientos, bodas, empleos, propiedades y más. Esa información se guarda a menudo en archivos públicos, lo que facilita a cualquiera un acceso inmediato. Y conforme crece el número de registros electrónicos, crece también la tendencia hacia una mayor accesibilidad a los datos personales.

El futuro de la reputación

Tan amplia exposición de datos personales disminuye la capacidad de proteger nuestra reputación mediante la configuración de la imagen que presentamos a los demás. La reputación desempeña un papel de suma importancia en nuestra sociedad; por lo que resulta esencial preservar los detalles íntimos de la vida propia. Consideramos la reputación de una persona para decidir si trabar o no amistad, acudir a una cita, contratarla o comprometernos en un eventual negocio con ella.

Podría aducirse que el declive de la privacidad potenciaría la desinhibición y la sinceridad de las personas. Pero si salen a la luz las transgresiones de todo el mundo, puede que las personas se juzguen unas a otras con mayor severidad. Que yo disponga de la información personal de otra persona puede que no mejore mi opinión sobre ella. Además, la pérdida de privacidad puede inhibir la libertad. La gran visibilidad que entraña la vida en un mundo transparente en línea acaso impida superar los errores pasados.

Las personas desean tener la oportunidad de "volver a empezar", de reinventarse a sí mismas de principio a fin. Tal como dijo en cierta ocasión John Dewey, una persona no es "algo completo, perfecto, [ni] acabado", sino "algo que se mueve, que cambia, diferenciado y, sobre todo, que empieza y no que acaba". En el pasado, los episodios juveniles de experimentación e insensatez terminaban olvidándose, ofreciendo la oportunidad de empezar de nuevo, cambiar y madurar. Pero con tanta información en línea, resulta más difícil olvidar esos momentos. La gente debe vivir ahora con el bagaje digital de su pasado.

Esa transparencia conlleva que las oportunidades para la "generación Google" se vean limitadas por culpa de algo que hicieron años atrás, en plena adolescencia. Sus más íntimos secretos podrían ser revelados por personas que ellos conocen. O podrían convertirse en víctimas involuntarias de un rumor falso. Guste o no, cada vez hay más información personal en la Red.

¿Qué hacer?

¿Podemos prevenir un futuro en que tanta información sobre la vida privada de las personas circule sin su control? Algunos tecnólogos y expertos legales dicen llanamente que no. La privacidad, sostienen, no es nada compatible con un mundo por donde la información fluye tan libremente. Innumerables libros y artículos han anunciado el "fin", la "muerte" y la "destrucción" de la privacidad.

Tales proclamas son, como mínimo, desatinadas. Resulta aún posible proteger la privacidad, pero ello requiere replantearse ciertas interpretaciones del concepto ya desfasadas.

Internet nunca olvida



FUENTE: VEOH

Un vídeo en YouTube puede provocar un ridículo a escala planetaria con la misma facilidad con que se pulsa la tecla "intro". En EE.UU., un joven que solicitaba un puesto de trabajo en una firma de inversiones envió su currículo acompañado de un vídeo. En éste, de título *Impossible is Nothing* ("Nada es imposible"), se veía al solicitante dedicado a proezas físicas variopintas, desde levantar 225 kilogramos en banco hasta ejecutar saltos de esquí y romper ladrillos a golpes de kárate. En todo el clip, el joven alardeaba de sus logros físicos y de su éxito general en la vida.

Huelga decir que el vídeo no se adecuaba especialmente al trabajo que pretendía el estudiante; y su arrogancia se veía tan desbordante, que el vídeo resultaba de lo más cómico. Parece que un trabajador de la empresa filtró el vídeo a Internet, donde cosechó éxito al instante; ya ha sido visto centenares de miles de veces. Por toda la Red, el estudiante ha sido objeto de burlas y parodias. Sus posibilidades de trabajo han disminuido de forma notable. Aunque desde luego cometió una equivocación y quizá le haya servido de lección, su juvenil bravata y error de apreciación ya están para siempre en el ciberespacio.

El autor

Daniel J. Solove es profesor de la facultad de derecho de la Universidad George Washington.

Una de ellas sostiene que la privacidad requiere el secreto total: una vez que una información se revela a otros, deja de ser privada. Esa idea sobre la privacidad resulta incompatible con un mundo en línea. Para las nuevas generaciones, la privacidad tiene más matices. Saben que la información personal se comparte de forma rutinaria con la de incontables otros, que dejan una estela de información por dondequiera que pasan.

La interpretación más sutil de privacidad de la generación Google reconoce que cada persona debe retener cierto control sobre la información personal que se pone a disposición pública. Esa generación desea dar su opinión acerca del modo en que se difunden los detalles de su vida privada.

El debate sobre el control de la información personal saltó al primer plano en 2006, cuando Facebook lanzó News Feeds, un producto que se encarga de enviar una notificación a los amigos de la persona registrada cuando el perfil de ésta cambia o se actualiza. Ante la sorpresa de los responsables de Facebook, muchos de los usuarios reaccionaron airados. Unos 700.000 se quejaron. A primera vista, la protesta contra News Feeds parece desconcertante. Muchos de los usuarios que protestaron tenían su perfil totalmente accesible al público. ¿Por qué creyeron que informar a sus amigos de los cambios en su perfil violaba la privacidad?

Para ellos la privacidad no implica ocultar secretos en un lugar remoto, pero sí poner límites a la accesibilidad. Imaginaron que la mayoría de la gente no escudriñaría los perfiles tan minuciosamente como para detectar cambios y actualizaciones leves, lo que les permitiría realizar cambios de forma inadvertida. Pero News Feeds de Facebook hacía que la información quedara a la vista. La objeción no fue, pues, sobre la ocultación de un secreto, sino sobre la accesibilidad al mismo.

En 2007 Facebook volvió a encontrarse con otra protesta sobre privacidad cuando lanzó un sistema de publicidad en dos partes, Social Ads y Beacon. Con Social Ads, siempre que un usuario escribía algo positivo acerca de un producto o un filme, Facebook usaba su nombre, imagen y palabras en anuncios publicitarios que se enviaban a los amigos; suponían que ese refrendo induciría a otros usuarios a adquirir un producto en mayor medida que un anuncio publicitario al uso. Con Beacon, Facebook estableció acuerdos para compartir bases de datos con numerosos sitios Web comerciales. Si una persona compraba por Internet una entrada de cine o un artículo, esa información salía de inmediato en el perfil público del individuo.

PRIVACIDAD: ESTRATEGIAS DE PROTECCION

La legislación estadounidense sobre privacidad es menos estricta que en otros países. El deseo de proteger en la Red la vida privada de las personas ha dado lugar a nuevas propuestas para conciliar la transparencia con la necesidad de restringir la publicación de datos personales.

Delito de apropiación
Los nombres y retratos (el rostro de Angelina Jolie, por ejemplo) no pueden emplearse, sin permiso, para conseguir beneficios económicos en anuncios publicitarios. Para luchar contra los abusos en línea, los supuestos de este delito podrían ampliarse para proteger frente a la publicación, sin permiso, de fotos en la Red.

Violación de la confidencialidad
Está protegida la información personal revelada en las relaciones confidenciales (a médicos, abogados y sacerdotes, entre otros). Las leyes contra esa clase de infracciones podrían reforzarse para que cubrieran otras relaciones (con amantes rechazados, ex amigos y ex cónyuges).

Privacidad en público
Según las leyes estadounidenses, ninguna persona retiene derechos de privacidad cuando una información se hace pública. En Canadá y numerosos países de Europa, esas revelaciones no implican la pérdida de tales derechos. En EE.UU. debería reconocerse que una persona no sacrifica todos sus derechos a la privacidad sólo por aparecer en público.

Facebook desplegó los programas sin informar debidamente a los usuarios, que se encontraron haciendo de señuelos publicitarios involuntarios en los sitios Web de sus amigos. Algunos se sintieron horrorizados al ver sus compras desplegadas en su perfil público de Facebook.

Las protestas y las consiguientes peticiones en línea reclamaban que Facebook modificara sus prácticas (el documento atrajo decenas de miles de firmas y resultó en varios cambios). Como testimonian esos casos, la privacidad debe limitar el acceso a los secretos. Los usuarios de Facebook no querían que se empleara su identidad para promocionar productos en Social Ads. Una cosa es escribir lo mucho que nos ha gustado una película o un disco compacto y otra muy distinta, que nos empleen en una valla publicitaria para presentar productos.

Cambiar las leyes

Canadá y la mayoría de los países europeos tienen una legislación sobre privacidad más rigurosa que EE.UU., que se ha resistido a promulgar una legislación integral. En otros lugares las leyes sobre privacidad reconocen que revelar información a otros no extingue el derecho propio a la privacidad. Pero el aumento de la accesibilidad a la información personal significa que la legislación estadounidense debe empezar a reconocer la necesidad de proteger un cierto grado de privacidad en la esfera pública.

En algunas áreas, la ley de EE.UU. dispone de mecanismos para controlar la información. El derecho de autor (*copyright*) reconoce unos derechos estrictos en la información pública que protegen una amplia gama de productos, desde filmes hasta programas informáticos. El derecho de propiedad intelectual no exige el confinamiento de un producto intelectual en un lugar inaccesible. Podemos leer una revista con *copyright*, sacar una copia para nuestro propio uso y prestársela a otros. Pero no podemos fotocopiarla de portada a portada o vender copias pirata en la calle. La legislación sobre la propiedad intelectual trata de lograr el equilibrio entre la libertad y el control, aun cuando debe seguir pugnando con las polémicas en curso en la era digital.

Lo más que la legislación estadounidense sobre privacidad se acerca a una doctrina legal sobre el *copyright* es mediante el delito de apropiación, que impide el uso del nombre o imagen de otro para obtener beneficios económicos. Por desgracia, esa legislación se ha desarrollado de modo que a menudo resulta ineficaz contra el tipo de amenazas a la privacidad que ahora proliferan. El *copyright* funciona

TOMMY MOORMAN

Mi vida es tu vida

Los usuarios de Facebook exigieron más protección a la privacidad después de que tres servicios enviaran información a “amigos” sin pedirles permiso.



TOMMY MOORMAN; FUENTE FACEBOOK (*captura de pantalla*)

principalmente como una forma de derecho de propiedad, que protege canciones, creaciones plásticas y otras obras de expresión personal.

Para hacer frente a las crecientes amenazas a la privacidad, deberían ampliarse los supuestos del delito de apropiación. Esa ampliación podría incorporar la interpretación original, de principios del siglo xx, de este principio del derecho consuetudinario anglosajón, que concebía la privacidad como algo más que un medio para proteger la propiedad: “El derecho a apartarse de la mirada pública en las ocasiones que cada persona pueda considerar adecuadas... está comprendido en el derecho a la libertad personal”, manifestó en 1905 el Tribunal Supremo de Georgia. Hoy, sin embargo, no se considera delito que la imagen o el nombre de una persona aparezca en sitios Web de noticias, arte, literatura o redes sociales. A la vez que protege el uso del nombre o la imagen de una persona para fines publicitarios, sin el permiso de esa persona, el delito de apropiación no comprende el empleo de esos elementos en reportajes periodísticos. Se trata de un matiz importante, pues significa que los comunicados de Internet rara vez serían delito.

Toda ampliación del alcance del delito de apropiación debe compaginarse con la contrapuesta necesidad de facilitar la labor de los servicios informativos y la difusión de información pública. Probablemente, debería considerarse que se produce delito sólo cuando se emplean fotografías u otra información personal, de modo que no respondan a un interés público, criterio que inevitablemente será objeto de las consiguientes deliberaciones judiciales.

La apropiación no es el único delito de derecho consuetudinario que precisa de una revisión general en esta era de comunicación digital. Disponemos ya de numerosas herramientas legales para proteger la privacidad, pero resultan inútiles por culpa de una concepción de la privacidad que les restan eficacia. La ampliación del marco legal debe tener en cuenta los usos problemáticos de la información personal, como los que ilustran el caso del chico de la *Guerra de las Galaxias* y el servicio Beacon de Facebook.

Lo mejor sería resolver tales disputas sin recurrir a los tribunales, pero la extensión que ha alcanzado la interconexión electrónica probablemente exigirá introducir cambios en la legislación. Las temibles amenazas que se ciernen sobre la privacidad realzan el valor fundamental de la misma. La sociedad debe desarrollar una nueva visión, con más matices, de la vida pública y la vida privada, una interpretación que reconozca el aumento de la información personal accesible y, no obstante, salvaguarde ciertas opciones acerca del modo en que se comparte y se distribuye esa información.

Bibliografía complementaria

PRIVACY AND FREEDOM. Alan Westin. Atheneum, 1967.

PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY. Ferdinand Schoeman. Cambridge University Press, 1984.

THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET. Daniel j. Solove. Yale University Press, 2007.

GUARDING LIFE’S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY. Lawrence M. Friedman. Stanford University Press, 2007.

UNDERSTANDING PRIVACY. Daniel J. Solove. Harvard University Press. 2008.

Ondas que guardan las formas

La transformación de la onda sonora inicial en un solitón, una onda que no se deforma, evita que un tren, al penetrar a gran velocidad en un túnel, genere una onda de choque de efectos desagradables

Jean-Michel Courty y Edouard Kierlik

Al entrar en un túnel, un tren de alta velocidad crea en el aire una sobrepresión que, al propagarse, se transforma en una onda de choque (*figura 1*). Para evitar a los pasajeros y a las poblaciones colindantes efectos tan molestos como las sacudidas sísmicas y los estallidos sónicos, se han propuesto diversas soluciones. La más original consiste en convertir la onda de choque en una "onda solitaria", menos agresiva. ¿De qué clase de onda se trata y cómo conseguirla? La propia luz nos lo aclara. Demos una vuelta por los solitones ópticos, impulsos lumínicos que recorren sin deformarse centenares de kilómetros de fibra óptica.

A la manera de un émbolo en un tubo, un tren que penetra en un túnel comprime de forma violenta el aire; la sobrepresión consiguiente se propaga a lo largo del túnel. En el interior de esa sobrepresión de unos 1000 pascal (una centésima de atmósfera), el aire está tanto más caliente cuanto más comprimido, o sea, cuanto mayor es la presión. Puesto que la velocidad del sonido aumenta con la temperatura, las distintas zonas de sobrepresión, que no se hallan a la misma temperatura, se desplazan a velocidades diferentes. La onda de sobrepresión se deforma entonces poco a poco: la zona más comprimida alcanza al frente delantero, igual que una ola a punto de romper (*figura 2*).

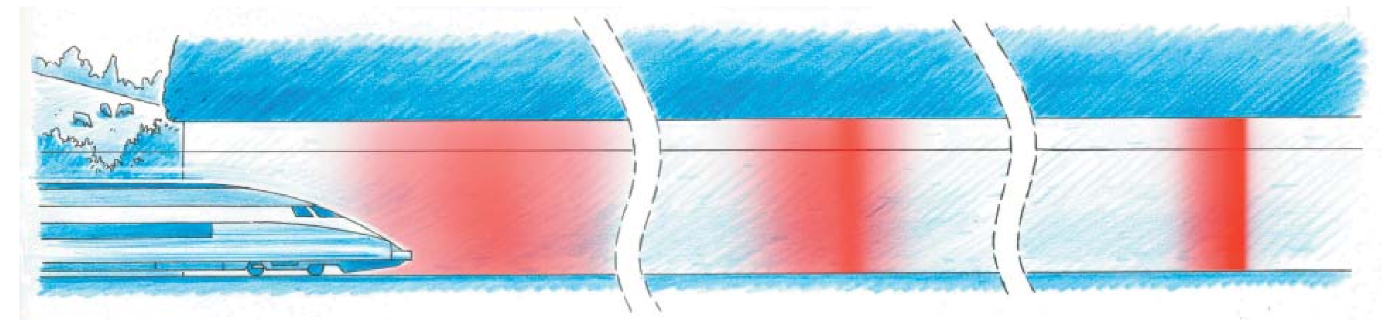
Al cabo de varios centenares de metros, la onda de sobrepresión se ha estrechado y su amplitud es casi el doble. Su frente se ha vuelto abrupto: se ha convertido en una onda de choque. Al final del túnel, la onda se refleja parcialmente hacia el tren, lo que resulta molesto para los pasajeros; en las tierras colindantes se oirá como un trueno.

Para que la onda de sobrepresión no se transforme en una de choque, habría que conseguir el equivalente acústico de un macareo (una ola que, durante las mareas más vivas, remonta los ríos sin romper). Esa clase de onda, que hoy se llama solitón, fue observada en 1834 por John Scott Russell, ingeniero de la marina escocesa. La detención súbita de una embarcación en un canal estrecho había creado una ola de unos 50 centímetros de altura y unos 10 metros de longitud que, para su sorpresa, no rompía. Russell la siguió a caballo (a diez de kilómetros por hora) durante cerca de un cuarto de hora, sin observar que su forma se alterase.

Macareos de luz

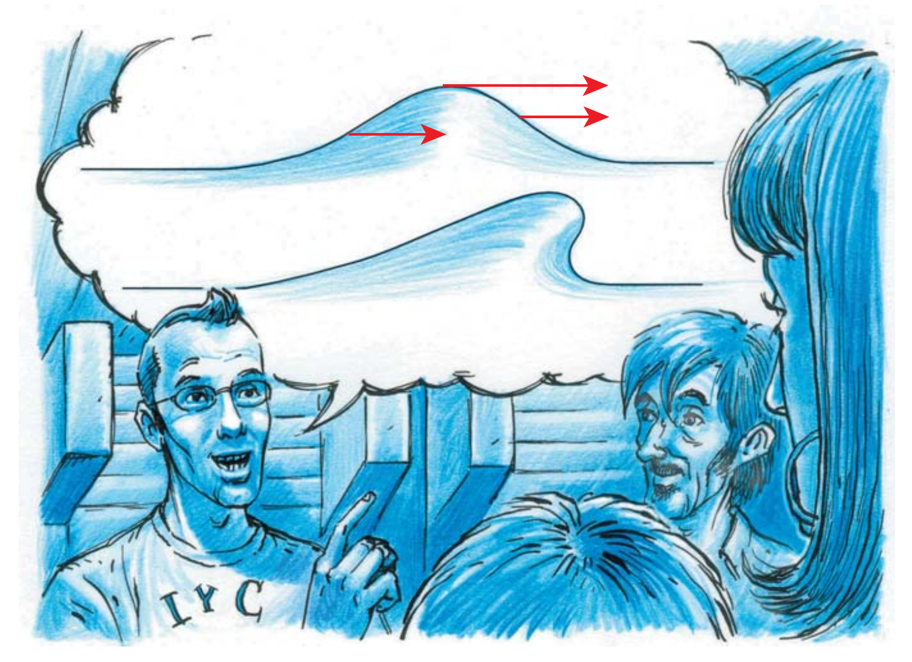
En un solitón se producen dos efectos adicionales compensatorios. El primero, opuesto al que hemos visto en la onda de sobrepresión, impide la estabilización de la onda. Para entenderlo, fijémonos en los solitones ópticos, impulsos luminosos de características peculiares que se propagan en las fibras ópticas. Lo mismo que la sobrepresión en un túnel, un impulso luminoso se deforma durante su progresión, ya que la velocidad de la luz en la materia depende de la intensidad de la onda. Además, la velocidad de la porción central del impulso es distinta de la velocidad en los flancos. Aun cuando ese efecto de no linealidad sea muy débil para las intensidades luminosas empleadas en las telecomunicaciones, al cabo de centenares de kilómetros de fibra se acumula y causa problemas: el impulso deformado amenaza con superponerse a los vecinos y producir errores en la transmisión de la señal.

Al revés que en la onda de sobrepresión aérea, la velocidad de propagación de la onda luminosa disminuye con la intensidad. Como la intensidad es máxima hacia el centro del impulso, esa zona avanza más lentamente que el frente delantero o trasero de la onda. Por consiguiente, las ondulaciones que forman la onda se estrechan en la parte trasera y se separan en la parte delantera; es decir, las longitudes de onda disminuyen en la parte posterior y aumentan hacia la parte anterior (*figura 3*).

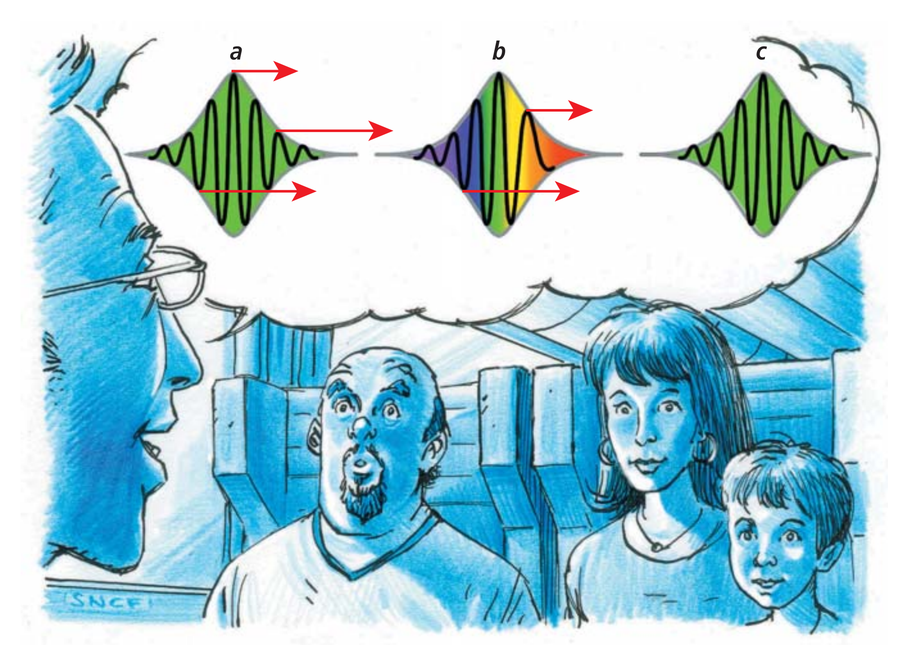


1. La velocidad del sonido aumenta con la temperatura. Ahora bien, en la zona central de la onda de sobrepresión (*izquierda*), la presión es máxima y el aire más caliente. Esa parte avanza con mayor prontitud que el frente delantero. Al cabo de dos o tres kilómetros, la zona central alcanza la parte delantera de la onda. La onda de sobrepresión se estrecha y se convierte en una onda de choque (*derecha*), en cuyo seno la sobrepresión casi se ha doblado.

ILUSTRACIONES DE BRUNO VACARO



2. La cresta de una ola que se acerca a la orilla viaja más rápido que las partes delantera y trasera (como en la onda de sobrepresión creada por un tren). Ello hace que la ola se deforme y acabe por desmoronarse, es decir, rompa. En un macareo, o solitón hidrodinámico, la dispersión (variación de la velocidad en función de la longitud de onda) compensa exactamente ese fenómeno.



3. En una fibra óptica, la parte intensa de un impulso luminoso avanza más lenta (*a*), lo que ensancha las ondulaciones en la parte delantera y, a la inversa, las estrecha en la parte posterior (*b*). Por otra parte, las longitudes de onda cortas se propagan a mayor velocidad que las largas (*b*). Cuando ambos efectos se compensan, se obtiene un solitón óptico, un impulso que conserva la forma (*a* y *c*).

El segundo efecto antagonista corresponde a la dispersión. En la materia, la velocidad de la luz depende de la longitud de onda. En el interior de una fibra óptica, la velocidad de propagación disminuye cuando aumenta la longitud de onda. Por tanto, el frente del impulso se propaga más lento que la cola. Poco a poco, las componentes de longitud de onda pequeña alcanzan y luego rebasan a las componentes de longitud de onda mayor, al revés que en el efecto anterior. Para una intensidad de onda elegida convenientemente, ambos efectos se compensan y crean un solitón óptico: un impulso luminoso que se propaga conservando la forma.

Ese solitón es un ente robusto. Si la intensidad inicial es excesiva, el impulso luminoso empieza por deformarse y perder parte de su energía, para formar finalmente un solitón que se propaga a lo largo de miles de kilómetros. Más aún, en una fibra óptica pueden inyectarse solitones de diferentes longitudes de onda. Estos se propagan a velocidades distintas y pueden, por tanto, colisionar. Sin embargo, sorprendentemente, tras la colisión los solitones recuperan su forma y su marcha, como si cada uno tuviera vida propia e independiente.

Largo tiempo considerada una utopía, la telecomunicación óptica por solitones es ya una realidad. Así, desde 2002 parte de las comunicaciones entre Córcega y el continente se efectúa mediante solitones que recorren 350 kilómetros de fibra óptica, sin repetidores submarinos, con una salida máxima de 800 gigabit por segundo y fibra.

¿Qué ocurre con el macareo? Por su parte, también se descompone en ondas de longitudes de onda diferentes, que se propagan a velocidades distintas. Igual que en el solitón óptico, su estabilidad la asegura la compensación entre dos efectos: la no linealidad ligada a la amplitud y la dispersión de las longitudes de onda.

Solitones sónicos

¿Y las ondas de sobrepresión en el aire? Puesto que la velocidad del sonido es la misma para todas las longitudes de onda, no se produce el efecto de dispersión. Esta es la razón de que no haya solitones naturales en acústica. ¿Cómo evitar entonces que la onda de sobrepresión creada por un tren no se deforme en onda de choque?

Nobumasa Sugimoto, de la Universidad de Osaka, ha dado con el modo de introducir la dispersión necesaria para formar un solitón acústico: instalar, a intervalos regulares en los costados del tubo, resonadores acústicos (simples cavidades) de las medidas adecuadas. Para las longitudes de onda próximas al valor correspondiente a una resonancia de las cavidades, la propagación se lentifica. Mediante la elección adecuada de las medidas de los resonadores, se consigue el efecto de dispersión deseado. Hasta el momento, las investigaciones se han limitado a tubos de diez metros de longitud, pero Sugimoto está convencido de que las cavidades ayudarán a poner a punto máquinas menos ruidosas (compresores, por ejemplo) y algún día permitirán transportar por vía acústica calor u otras formas de energía.

Los desafíos del nuevo Zenón

Cómo interactuar con un número infinito de obstáculos sin interactuar con ninguno en particular

Gabriel Uzquiano

Queremos desplazarnos de un punto A a un punto B. Uno de los argumentos que se le atribuyen a Zenón de Elea sugiere que nos encontramos ante una tarea imposible. Llamemos A_1 al punto intermedio entre A y B. Para completar nuestro desplazamiento deberíamos haber completado antes el trayecto entre A_1 y B. Llamemos A_2 al punto intermedio entre A y A_1. Para completar la tarea anterior deberíamos haber completado antes el trayecto de A_2 a A_1. Llamemos A_3 al punto intermedio entre A y A_2, etcétera. En general, para completar el desplazamiento de A a B deberíamos haber completado antes un número infinito de tareas. Deberíamos haber completado el traslado de A_1 a B, el traslado de A_2 a A_1, el traslado de A_3 a A_2, etc. Ahora bien, razonaría Zenón, si agregáramos todos los intervalos de tiempo que necesitaríamos invertir en cada uno de los traslados, nos encontraríamos ante una suma infinita cuyo valor debería ser infinito. ¿Cómo podrían seres finitos como nosotros invertir un período infinito de tiempo en el trayecto de A a B?

Uno se siente inclinado a responder a Zenón según hiciera Diógenes el cínico en su día: levantándose y, sin mediar palabra, echando a andar. Como recoge el dicho, "el movimiento se demuestra andando". Sin embargo, la respuesta de Diógenes, transmitida por Aristóteles, no llega a explicarnos dónde se encuentra el error en el razonamiento.

¿Quiere saber más?

La paradoja de los dioses se formuló en *Infinity: An Essay in Metaphysics*, por J. Bernardete. Clarendon Press; Oxford , 1964. En este libro se discuten variaciones aún más desconcertantes del argumento originalmente atribuido a Zenón.

Para una discusión general de las paradojas de Zenón, recomiendo *Paradoxes*, por M. Sainsbury. Cambridge University Press; Cambridge, 1988.

Quizá sea más iluminador apuntar, tal como hiciera Aristóteles, que los intervalos requeridos para completar cada tramo son cada vez más breves: la mitad del total para el tramo final, un cuarto del total para el tramo previo, un octavo para el tramo inmediatamente anterior, etc. ¿No nos encontramos todavía ante una suma infinita de intervalos finitos? Sí, así es. ¿No debería la suma tener un valor infinito como resultado? No, no necesariamente. Contamos desde finales del siglo XIX con las herramientas necesarias para calcular la suma de una serie infinita de términos. Digamos, en general, que la suma de una serie infinita $\{s_n\}$:

$$s_1, s_2, s_3, s_4, \ldots$$

es el límite de la serie infinita de sumas parciales $\{S_n\}$:

$$S_1 = s_1$$
$$S_2 = s_1 + s_2$$
$$S_3 = s_1 + s_2 + s_3$$
$$\ldots$$
$$S_n = s_1 + \ldots + s_n$$

siempre que tal límite exista. En el caso que nos ocupa, los términos de la serie $\{s_n\}$ son:

$$1/2, 1/4, 1/8, 1/16, \ldots$$

de modo que las sumas parciales son las siguientes:

$$1/2 = 1/2$$
$$1/2 + 1/4 = 3/4$$
$$1/2 + 1/4 + 1/8 = 7/8$$
$$1/2 + 1/4 + 1/8 + 1/16 = 15/16$$
$$\ldots$$

Pero esta serie de sumas parciales tiene a 1 como límite. Decir que el límite de una serie infinita es 1 no es más que decir que la diferencia entre 1 y los sucesivos términos de la serie va disminuyendo progresivamente hasta caer por debajo de cualquier valor por mínimo que sea éste. Formalmente, el límite de una serie infinita $\{s_n\}$ es l si para todo $\varepsilon > 0$, hay algún número positivo n tal que para todo $m > n$, la diferencia entre l y s_m sea menor que ε. Pero dado cualquier valor ε, es posible encontrar un término t_n en la serie:

$$1/2, 3/4, 7/8, 15/16, 31/32, \ldots$$

tal que la diferencia entre 1 y todo término por encima de t_n sea menor que ε. En resumen, no es cierto que el resultado de la suma de los términos de una sucesión infinita deba ser infinito.

Alguien podría objetar que el problema fundamental radica, no en el intervalo de tiempo que uno requiere para completar las tareas, sino en el hecho de que se trate de un número infinito de tareas. ¿Cómo podrían seres finitos como nosotros realizar un número infinito de tareas? Aunque la respuesta de Diógenes pueda venir a la mente, lo cierto es que esta cuestión es todavía objeto de intenso debate entre filósofos. Un problema diferente surge cuando uno se pregunta qué tarea realizar primero. Parece que no es posible llevar a cabo una de ellas, a menos que se hayan llevado a cabo un número infinito de tareas previas. Este segundo problema es el que vamos a explotar a fin de plantear los desafíos del nuevo Zenón.

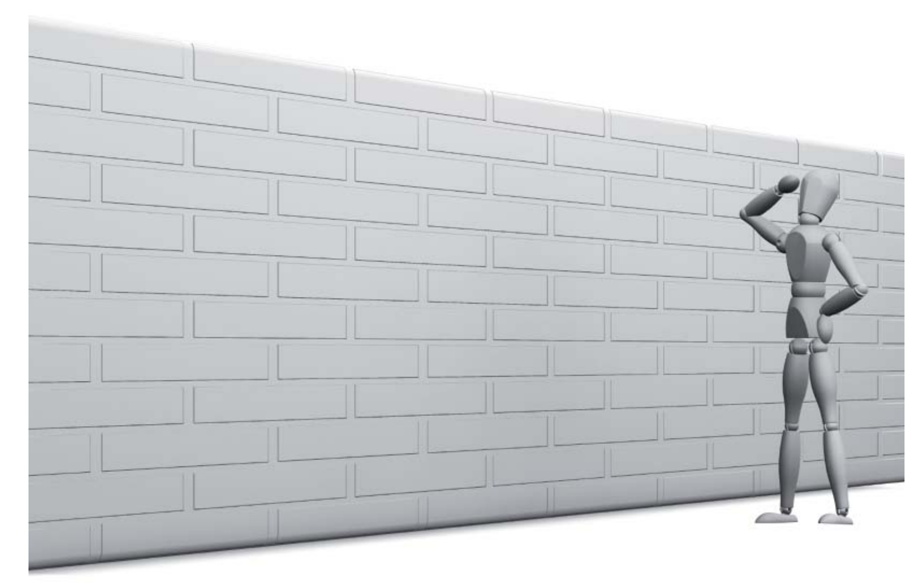
Queremos desplazarnos de nuevo de A a B, que ahora se encuentran a un kilómetro de distancia. Esta vez nos enfrentamos a las intenciones de un número infinito de dioses empeñados en impedir nuestro desplazamiento. Un dios quiere impedir nuestro traslado a toda costa y, para ello, va a levantar un muro en A_1, el punto intermedio entre A y B, si (pero sólo si) constata nuestro avance más allá de A_2, que se encuentra en el primer cuarto de kilómetro. Un segundo dios que desconoce las intenciones del primero está dispuesto a impedir nuestro avance levantando un muro en A_2, que se encuentra en el primer cuarto de kilómetro, si (pero sólo si) constata nuestro avance más allá de A_3, que se encuentra en el pri-

mer octavo de kilómetro. Un tercer dios, que desconoce las intenciones de los dos primeros, está dispuesto a impedir nuestro avance levantando un muro en A_3, que se encuentra en el primer octavo de kilómetro, si (pero sólo si) constata nuestro avance más allá de A_4, que se encuentra en el primer dieciseisavo de kilómetro. Un cuarto dios... Tenemos así un número infinito de dioses dispuestos a impedir nuestro desplazamiento y con la siguiente característica: el enésimo dios está dispuesto a levantar un muro en el punto A_n que se encuentra en el primer $1/2^n$ de kilómetro una vez constate nuestro avance más allá de A_{n+1}, que se encuentra en el primer $1/2^{n+1}$ de kilómetro.

Parece evidente que no podemos contrariar a todos los dioses, de manera que deberíamos permanecer inmóviles en el punto de partida. Pero supongamos que no nos vamos a detener a menos que alguien impida nuestro avance. ¿Qué dios detendrá nuestro avance? No será el primer dios, ya que éste no tomará cartas en el asunto a menos que consigamos llevar a cabo un cuarto del desplazamiento. Pero tampoco será el segundo, ya que éste no tomará cartas en el asunto a menos que consigamos llevar a cabo un octavo del desplazamiento. Tampoco será el tercero... Pero si ningún dios nos impide el avance hacia *B*, deberíamos poder progresar hacia *B*.

No es consuelo pensar que las leyes de nuestro mundo podrían ser incompatibles con la existencia de agentes capaces de tener y de ejecutar las intenciones descritas en el ejemplo. Nos basta con que sea posible que existan agentes con las capacidades e intenciones apropiadas en algún mundo posible. Ni es mayor consuelo añadir que aunque tales agentes fueran genuinamente posibles, el mundo resultante sería tan diferente del nuestro como para que no nos preocupe excesivamente lo que ocurra en él. A veces son los mundos más distantes los que nos permiten iluminar la naturaleza de nuestros conceptos.

Tal vez la solución sea negar que nos encontramos ante una descripción coherente. Podemos compararla con la descripción de una situación en la que dos agentes no sólo tienen, sino que llevan a cabo, la intención de escribir un número mayor que el número escrito por el otro. Aunque no hay problema en asumir que ambos agentes puedan tener la intención en cuestión, parece obvio que no hay una situación en la cual ambos puedan ejecutarla simultáneamente. Tal vez deberíamos concluir que, aunque un número infinito de dioses pueda tener las intenciones descritas en nuestro ejemplo, no hay una situación coherente en la cual todos ellos cumplen con su palabra. No es que haya un dios en particular que no pueda cumplir su palabra. Lo que no puede ocurrir es que lo hagan todos simultáneamente.



Siguiente desafío. Queremos desplazarnos de nuevo de *A* a un punto *B* que se encuentra a un kilómetro de distancia. Esta vez nos enfrentamos a un número infinito de obstáculos en nuestro camino. Nos enfrentamos en A_1 a un muro infranqueable de un metro de grosor. En A_2, que se encuentra a un cuarto de kilómetro de *A*, nos enfrentamos a un muro infranqueable de medio metro de grosor. En A_3, que se encuentra a un octavo de kilómetro de *A*, nos enfrentamos a un muro infranqueable de un cuarto de metro de grosor. En A_4, que se encuentra a un octavo de kilómetro de *A*... Parece evidente que no vamos a poder superar todos los obstáculos, de modo que no hay esperanza de alcanzar *B*. Por otra parte, parecería que no nos detendríamos hasta que no entrásemos en contacto con uno de los muros.

¿Qué muro detendrá nuestro avance? No será el primero, ya que no entraremos en contacto con él a menos que superemos un número infinito de obstáculos previos. Tampoco será el segundo, ya que no entraremos en contacto con él a menos que superemos un número infinito de obstáculos previos. No será el tercero... Pero si ningún muro detiene nuestro avance, parece que deberíamos poder progresar en nuestro avance hacia *B*.

No podemos apelar a la distinción entre tener una intención y encontrarse en posición de ejecutarla, ya que los muros carecen de intenciones o de la habilidad de ejecutarlas. Pero entonces, ¿cómo se resuelve problema? Una opción es la siguiente. Pensemos en la suma de todos los muros. Este es un objeto que tiene como partes el primer muro, el segundo muro, el tercer muro, etcétera, y no tiene ninguna parte que no sea parte de uno de los muros. La suma de los muros es diferente de todos y cada uno de los muros individuales y ocupa cada una de las regiones ocupadas por los muros. Además, *A* es lo que se conoce como punto de acumulación del conjunto de regiones ocupadas por cada uno de los muros individuales. Todo intervalo centrado en *A* contiene puntos pertenecientes a una de las regiones ocupadas por los muros.

Tal vez la solución a nuestro problema consista en decir que, aunque no nos encontremos en contacto con ninguno de los muros, nos encontraremos en contacto con la suma de los mismos. ¿Por qué? Porque al fin y al cabo no hay un solo punto que separe *A* de la suma de los muros. Dado un punto C cualquiera entre *A* y *B* existe un punto A_n ocupado por la suma de los muros que se encuentran más próximos a *A* que *C*. A veces es posible entrar en contacto con una suma de objetos sin entrar en contacto con uno de ellos.

No está todo dicho. Hay variaciones aún más desconcertantes del razonamiento de Zenón que hemos de dejar para otra ocasión.

Revelado instantáneo

Colores en seco

Mark Fischetti

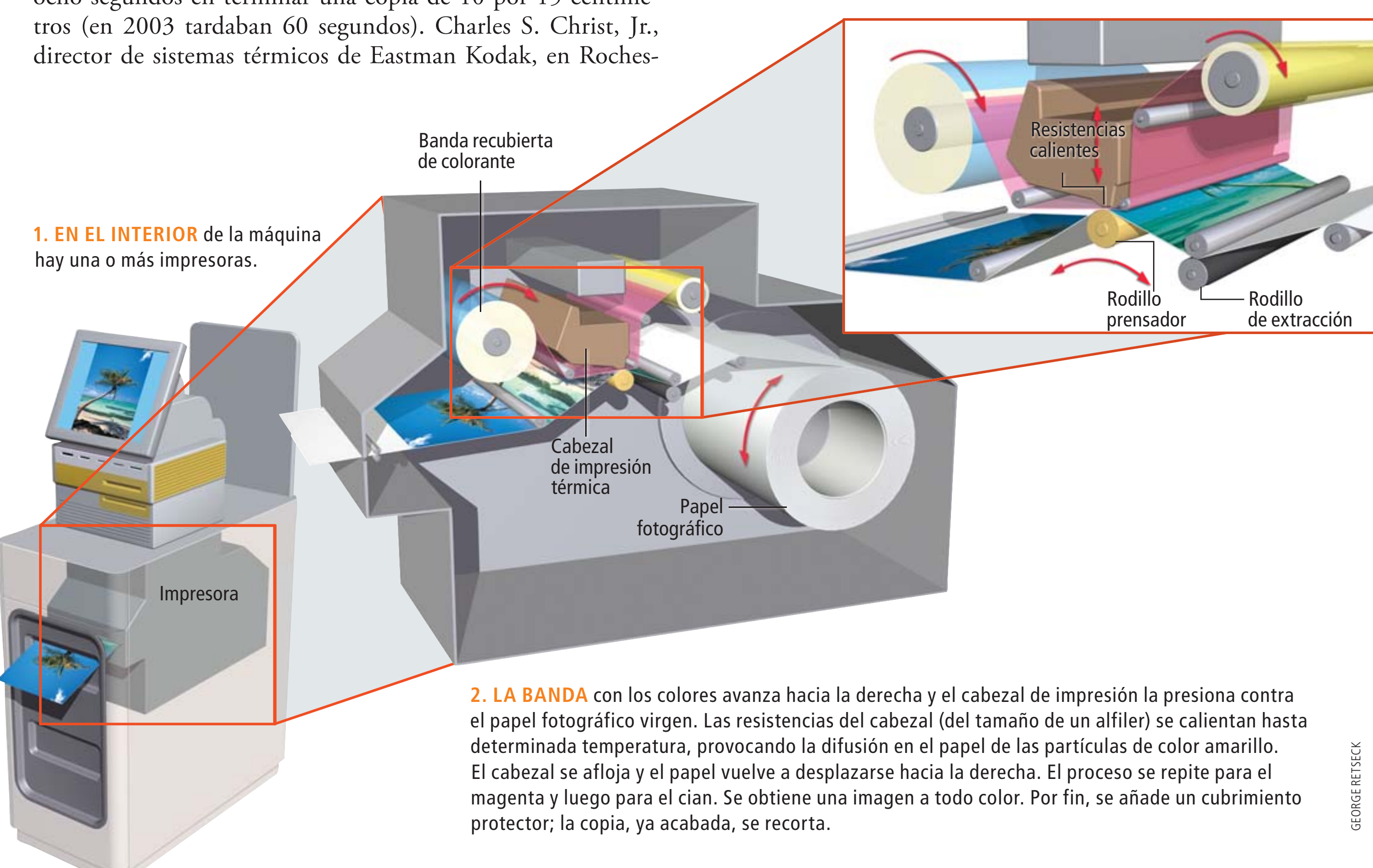
El constante auge de la fotografía digital ha propiciado el rápido crecimiento de una nueva industria: el revelado instantáneo. Nuestra entusiasta fotógrafa, harta ya de pulsar el disparador, lleva la tarjeta de memoria de su cámara a un establecimiento comercial, la introduce en un quiosco de revelado y elige las fotos que desea. Instantes después salen las copias por la rampa. Parecen omnipresentes esas máquinas. En cinco años, el número de quioscos de revelado digital se ha disparado hasta 85.000 en todo el mundo.

Estos dispositivos hacen uso de una técnica de revelado "en seco": la impresión por transferencia térmica (distinta del método tradicional "húmedo", basado en la acción de baños químicos). Conforme el papel fotográfico avanza por delante del cabezal de impresión, unas diminutas resistencias dispuestas en hilera se calientan cada una hasta una temperatura determinada, transfiriendo minúsculas cantidades de pigmento amarillo, magenta o cian, desde una banda al papel. En conjunto, las manchitas forman píxeles de color.

Las máquinas de mayor tamaño que operan en los centros de revelado usan también la electrofotografía, sobre todo para trabajos a dos caras, como tarjetas de felicitación o calendarios personalizados, ya que la resolución es inferior a la del método térmico. Las máquinas térmicas actuales tardan unos ocho segundos en terminar una copia de 10 por 15 centímetros (en 2003 tardaban 60 segundos). Charles S. Christ, Jr., director de sistemas térmicos de Eastman Kodak, en Rochester (Nueva York), afirma que los quioscos de revelado del futuro serán aún más rápidos.

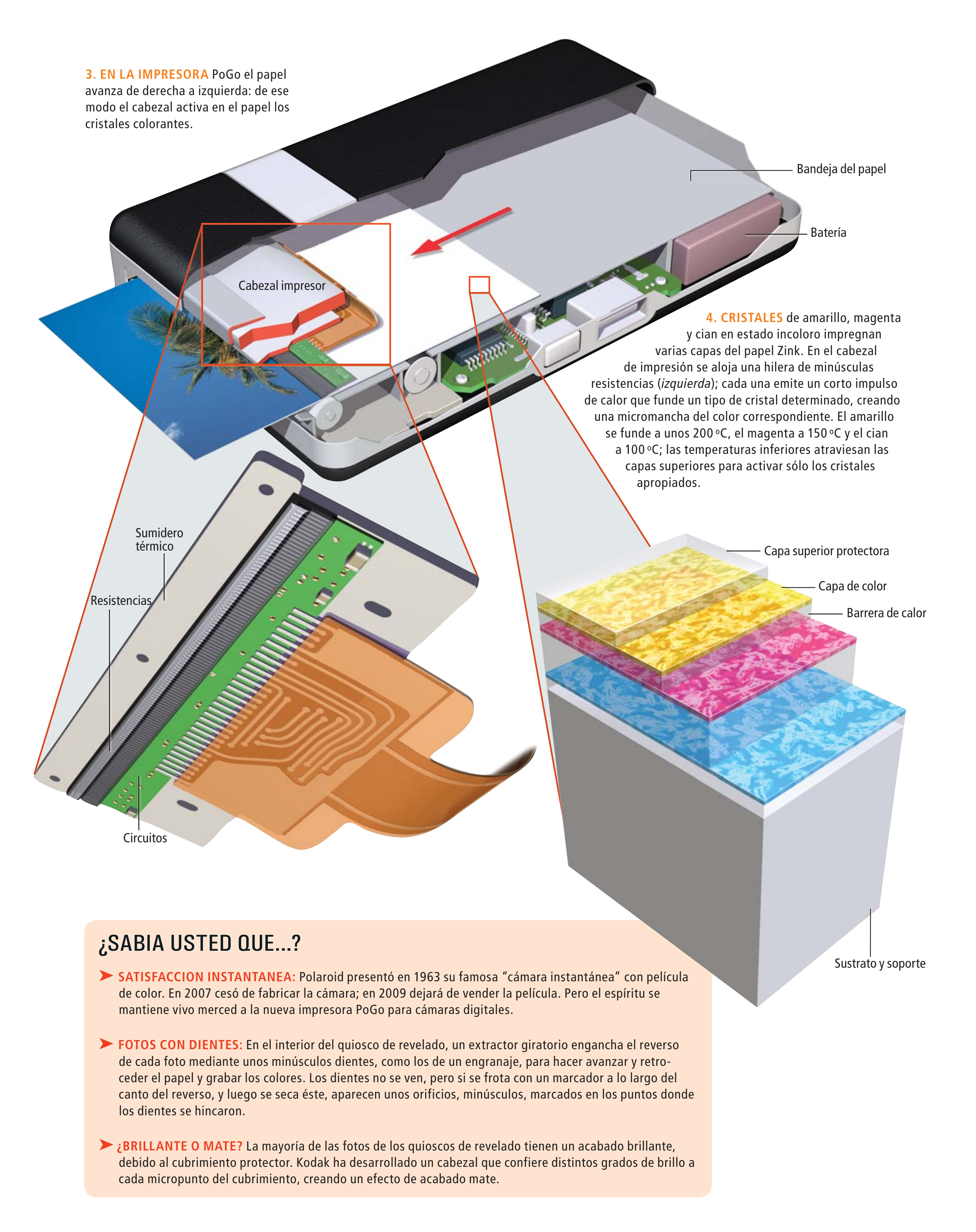
Una forma extrema de revelado en seco está volviendo a poner de moda la "foto instantánea". En julio, Polaroid presentó la PoGo, una impresora portátil de bolsillo que hace copias de 5 por 7,5 centímetros procedentes de una cámara digital, bien mediante una conexión inalámbrica Bluetooth o un cable USB. El método lo ha desarrollado Zink Imaging, una empresa de nueva creación con sede en Bedford (Massachusetts); Stephen Telfer, director de investigación de la compañía, es el inventor de la parte química.

En el sistema PoGo, se incrustan en el papel fotográfico cristales incoloros, que, cuando se calientan mediante las resistencias del cabezal de impresión, se tornan amarillos, magenta o cian. La PoGo imprime una imagen en 60 segundos, funciona con baterías y puede emplearse en cualquier situación: fiestas, vacaciones y eventos empresariales, todas en el punto de mira de Polaroid. Los primeros ejemplares se vendían a 100 euros, y a 7 euros las 30 hojas de papel. Informa Telfer de que existen ya en fase de prototipo copias de mayor tamaño. Asimismo, dado que esas impresoras no usan tinta, podrían instalarse en aparatos electrónicos, como un televisor, para sacar copias de las imágenes de la pantalla.



1. EN EL INTERIOR de la máquina hay una o más impresoras.

2. LA BANDA con los colores avanza hacia la derecha y el cabezal de impresión la presiona contra el papel fotográfico virgen. Las resistencias del cabezal (del tamaño de un alfiler) se calientan hasta determinada temperatura, provocando la difusión en el papel de las partículas de color amarillo. El cabezal se afloja y el papel vuelve a desplazarse hacia la derecha. El proceso se repite para el magenta y luego para el cian. Se obtiene una imagen a todo color. Por fin, se añade un cubrimiento protector; la copia, ya acabada, se recorta.

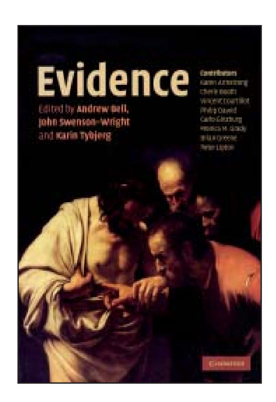


¿SABIA USTED QUE...?

➤ **SATISFACCION INSTANTANEA:** Polaroid presentó en 1963 su famosa "cámara instantánea" con película de color. En 2007 cesó de fabricar la cámara; en 2009 dejará de vender la película. Pero el espíritu se mantiene vivo merced a la nueva impresora PoGo para cámaras digitales.

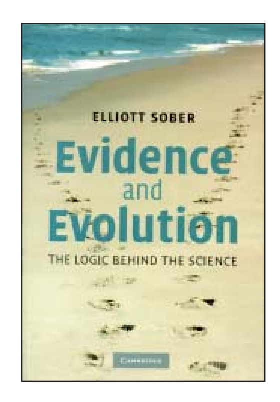
➤ **FOTOS CON DIENTES:** En el interior del quiosco de revelado, un extractor giratorio engancha el reverso de cada foto mediante unos minúsculos dientes, como los de un engranaje, para hacer avanzar y retroceder el papel y grabar los colores. Los dientes no se ven, pero si se frota con un marcador a lo largo del canto del reverso, y luego se seca éste, aparecen unos orificios, minúsculos, marcados en los puntos donde los dientes se hincaron.

➤ **¿BRILLANTE O MATE?** La mayoría de las fotos de los quioscos de revelado tienen un acabado brillante, debido al cubrimiento protector. Kodak ha desarrollado un cabezal que confiere distintos grados de brillo a cada micropunto del cubrimiento, creando un efecto de acabado mate.



EVIDENCE.

Dirigido por Andrew Bell, John Swenson-Wright y Karin Tybjerg. Cambridge University Press; Cambridge, 2008.



EVIDENCE AND EVOLUTION. THE LOGIC BEHIND THE SCIENCE,

por Elliott Sober. Cambridge University Press; Cambridge, 2008.

Prueba

Criterio determinante del método científico, no puede asegurar la certeza de una teoría

Las pruebas constituyen un elemento central del método científico. Con ellas nos convencemos y con ellas intentamos convencer. A veces, su contundencia es inmediata. En su *Robinson Crusoe*, Daniel Defoe presenta un ejemplo nítido del poder de la prueba: creyéndose solo en una isla, Crusoe descubre pisadas humanas en la arena. Su vida cambió de repente y se aprestó a descubrir al autor de las huellas. Las pruebas revisten múltiples formas. Cada disciplina, si no cada problema, reclama la suya propia: observación, estadística, documentos, experimentos, coherencia matemática, normas o reglas de razonamiento, etcétera (*Evidence*). Cuando se habla de método científico, la prueba, o contrastación empírica, aparece de inmediato como el criterio último y discriminante de cientificidad. De ahí la tendencia a considerarla algo fijo e inmutable, una suerte de fulcro arquimideano sobre el que se apoya el conocimiento científico. Pero se trata sólo de una meta, pues nuestro conocimiento actual de la inferencia científica es fragmentario.

En efecto, la naturaleza y función de la prueba pueden abordarse en relación con una disciplina particular (la prueba en biología o en física) o pueden abordarse en términos generales, desde la perspectiva de la filosofía de la ciencia. En epistemología, la cuestión de la prueba se encuadra en el capítulo sobre la posibilidad de conocimiento. Nuestras ideas sobre el mundo se han comparado con una red extensa. Esa red evoluciona con el tiempo. Y lo hace por doble vía: interna y externa. En evolución externa, la red crece mediante adición de nuevas ideas que provienen de fuera, verbigracia, cuando vemos objetos nuevos y cuando admitimos el testimonio de otro. En evolución interna, se produce adición de nuevas ideas a través de la inferencia. Las pruebas nos llevan a la inferencia, a la formación de nuevas ideas a partir de otras ya asentadas. Procede así el paleontólogo cuando, al desenterrar un fósil, infiere que se trata de un dinosaurio que vivió hace millones de años; el astrónomo que, cuando observa que el espectro característico de la galaxia se corre hacia el rojo, infiere que ésta se aleja de nosotros a una velocidad particular; etcétera.

¿De qué modo las ideas existentes en la red determinan qué nuevas ideas deben añadirse? ¿Cómo decidimos el camino en que apunta la prueba? ¿Aplicamos correctamente la prueba? A las nuevas ideas se les exige, de entrada, que sean verdaderas. La verdad de la prueba garantiza la corrección de la inferencia o deducción. (En la deducción, la verdad de las premisas, la prueba, garantiza la verdad de la conclusión, la inferencia. Si las premisas son verdaderas, la conclusión debe ser verdadera; de forma equivalente, es imposible que las premisas sean verdaderas y la conclusión sea falsa.) Cuando extraemos consecuencias que van más allá de las consecuencias lógicas, partimos del supuesto de que en el futuro las cosas serán iguales que hoy. Esperamos más de lo mismo. Pero no podemos estar nunca absolutamente seguros de que acontecerá eso. No importa cuántas veces sale el Sol, no existe garantía de que así sucederá mañana. La deducción no nos permite extraer inferencias sobre qué sucederá en el futuro a partir de las pruebas sobre lo que aconteció en el pasado.

Esas inferencias no demostrativas son inferencias inductivas. A menudo hacemos predicciones que resultan ser incorrectas, pese a ser correctas las observaciones en que se basaron, lo que no significa negar valor a las pruebas inductivas. Cierto es que la inducción se resiente todavía del juicio severo que emitió David Hume. Para Hume, cuando extendemos nuestro conocimiento mediante la inferencia inductiva, cometemos una extrapolación. En esa suerte de "más de lo mismo", vemos una pauta en el mundo y predecimos que la pauta ha de continuar. Pero lo que sucedió en el pasado no tiene por qué acontecer en el futuro. No ha lugar, pues, a la inferencia inductiva. El hombre, razonaba, es una criatura formadora de hábitos y, al observar que una cosa sigue a otra determinada, termina por esperar que la segunda aparezca cuando se dé la primera.

Las pruebas que los científicos reúnen para avalar sus teorías no hacen ciertas las teorías. La ciencia es falible. Las teorías suelen abarcar un ámbito más general que el conseguido con las pruebas que nos llevan a ellas. En física, la teoría general de la relatividad y la mecánica cuántica formulan enunciados sobre lo que es verdadero en todos los tiempos del universo entero; nuestras observaciones, sin embargo, se encuentran limitadas a una porción muy restringida de esa totalidad inmensa. De lo que sucede aquí y ahora (y en sus aledaños) no se infiere deductivamente lo que acontece en lugares remotos y en tiempos muy distantes del nuestro. Si las pruebas que la ciencia reúne no permiten declarar qué teorías son verdaderas, ¿para qué sirven las pruebas? ¿Cuál es la relación entre prueba y teoría?

En biología evolutiva, Elliott Sober lo tiene muy claro. Sober fija el carácter probabilístico, bayesiano, de la prueba en los procesos de selección natural y procedencia de un antepasado común (*Evidence and Evolution*). Para declarar qué enunciados son *probablemente* verdaderos, distingue entre bayesianos, frecuentistas y "partidarios de la verosimilitud". Defiende que el bayesianismo resulta idóneo para muchas inferencias científicas; aunque esté de acuerdo con los frecuentistas al reconocer que la aplicación de los métodos bayesianos en otros contextos se hace problemática; predíquese lo mismo de los criterios frecuentistas, muy débiles. El bayesianismo se propone responder a la pregunta "¿qué es lo que debemos aceptar?" Es decir, aborda la cuestión de cuán seguros podemos estar de que el paciente tiene tuberculosis, considerando que el test de la tuberculosis resultó positivo. Aunque el bayesianismo se apoya en el teorema de Bayes, constituye en realidad una teoría filosófica, una epistemología.

Un ejemplo de la diferencia de pruebas entre materias distintas nos lo ofrece Vincent Courtillot con el caso particular de las catástrofes globales, que pone en jaque a la paleontología, la biología y la geología, ciencias esencialmente históricas y que, en cuanto tales, divergen de la física y la química. Las pruebas pueden llegar de la observación de las rocas o de restos fósiles desenterrados en el campo; pueden proceder también de experimentos realizados en el laboratorio o de mediciones emprendidas en el laboratorio sobre especímenes recuperados en el campo; pueden también proceder de simulaciones numéricas que están adquiriendo una importancia creciente merced al avance de la computación. Pueden considerarse, por último, resultado de razonamiento lógico o como construcción de un modelo y su contrastación, apoyado en otros tipos de pruebas enumerados antes.

Las pruebas tomadas de la paleontología son siempre un tanto ambiguas. Si se descubre un hueso fósil y lo atribuimos a una especie extinta no significa que sea el último individuo de la especie extinguida; la especie pudo demorar milenios su desaparición sin dejar ningún resto fósil. Tenemos que esforzarnos por descubrir las causas de acontecimientos raros, como las extinciones masivas (tanto, que la última ocurrió hace 65 millones de años). A lo largo del siglo pasado se esbozaron más de un centenar de hipótesis sobre las extinciones en masa. De ellas han quedado tres o cuatro, que toman por ejemplo arquetípico la extinción del Cretácico-Terciario (la de los dinosaurios). Fijémonos en las dos preeminentes. La primera, planteada por Luis y Walter Alvarez en 1980, sostiene que un meteorito chocó contra la Tierra hace 65 millones de años, arrojando cantidades ingentes de polvo en la atmósfera y desencadenando un invierno nuclear. Este habría venido acompañado de grandes incendios y de un clima de efecto invernadero en razón de la acumulación de dióxido de carbono en la atmósfera. La segunda hipótesis postula un episodio de erupción volcánica más o menos coetánea con el impacto del meteorito.

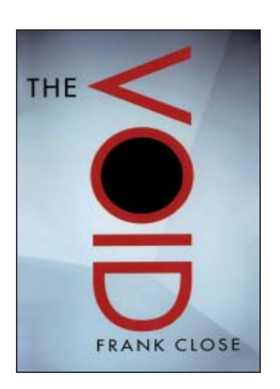
Para Courtillot, la acción volcánica podría explicar de una manera más cabal el alcance y la extensión de la extinción.

Los episodios eruptivos concuerdan con la extinción contemporánea; queda

paladino por la ausencia de fósiles en las capas estratigráficas, mientras que el impacto del meteorito concuerda bien con la capa de iridio y un episodio imponente de extinción en masa. La segunda cuestión es: ¿qué decir de las otras extinciones en masa? La correlación entre la edad de los flujos de basalto y la edad de las extinciones en masa ha ido refinándose con el estudio de los últimos años. Parece cada vez más claro que las grandes extinciones en masa han coincidido con episodios de vulcanismo. En cambio, se han producido numerosos impactos en la historia de la Tierra sin que le haya acompañado una catástrofe biogenética. Con una única salvedad: el impacto mexicano coincide con una extinción en masa, la de hace 65 millones de años. Pero ese impacto se produjo cuando ya venían sucediéndose episodios de vulcanismo varios cientos de miles de años antes. Parece, pues, razonable proponer que la extinción coincidente en el tiempo con un impacto recibió un impulso amplificador por un entorno sometido a tensión y que había dado ya los primeros pasos en la extinción en masa. Si el meteorito hubiera caído en tiempo de un vulcanismo no extremo, tal vez no hubiera dejado rastro en el registro paleontológico. La coincidencia entre vulcanismo y extinción constituye un indicio sólido, pero no la prueba final. La fase siguiente estribará en reconstruir la cadena real de episodios físicos en cuya virtud un vulcanismo extremo desencadena la muerte de especies e individuos.

¿En qué prueba basarse cuando hablamos de vida extraterrestre? Lo más sensato es partir de lo que conocemos sobre la vida terrestre. Sensatez que se funda en el supuesto de que las reglas físicas y químicas que gobiernan la vida sobre la Tierra necesariamente deben ser su soporte en cualquier parte del universo. La posibilidad lógica de que la vida encuentre su camino en ambientes extremos abre infinitas posibilidades para la lucubración. Lo que obliga a considerar las condiciones de la biosfera, los límites que definen las posibilidades de vida en la Tierra, para indicar lo que podría ocurrir en otros sitios. Ha aparecido vida en lugares inhóspitos, a temperaturas por encima del punto de ebullición y por debajo del punto de congelación. Hemos sabido de la posible presencia de agua en Marte, planeta cuya superficie guarda ciertas semejanzas con la Antártida, donde se ha descubierto una biomasa importante de líquenes y otros organismos elementales. De igual modo, el descubrimiento de ecosistemas exitosos en los humeros hidrotermales en el lecho oceánico, basados en la energía química y no en la fotosíntesis y el oxígeno, anima la investigación sobre posibilidades de vida en otros océanos profundos, como el de Europa, satélite de Júpiter.

Luis Alonso



THE VOID,
por Frank Close.
Oxford University Press; Oxford, 2007.

Vacío

Cuando se promete más de lo que se ofrece, o quien mucho abarca poco aprieta

La nada, ¿es algo? Esta pregunta intrigante ha captado la atención de un gran número de pensadores. En Occidente, desde que los filósofos griegos intentaran darle una respuesta racional, ha sido una cuestión recurrente. Ya en nuestros días, el desarrollo de la mecánica cuántica abre nuevos horizontes. Dicho de manera abreviada, el principio de indeterminación impone que incluso la energía del nivel más bajo al que se pueda llegar no sea exactamente nula. Lo cual implica que incluso en el vacío hay algo, y por lo tanto la nada sería una entelequia inalcanzable.

Precisamente los experimentos que ahora se están desarrollando en el CERN, el centro europeo de física de partículas, intentan dilucidar cuál es el origen cuántico de la masa, un tema relacionado con el que se propone en esta obra. Para ello, los investigadores van a tratar de detectar el bosón de Higgs, una partícula cuya existencia fue propuesta hace ya tiempo pero que sólo ahora está —por lo que parece— al alcance de los experimentos.

El libro traza un recorrido por las grandes concepciones humanas del universo: los clásicos de la antigua Grecia, Newton, Einstein, la mecánica cuántica... Quizá sea éste su gran atractivo, y a la vez el mayor defecto. El autor describe con viveza los enigmas más acuciantes de cada época, y resume las teorías científicas con magistral brevedad, sin perder exactitud. De manera que se lee con la misma voracidad que una novela de intriga, y resulta accesible incluso a quienes no posean más que un somero bagaje científico o matemático. Bien es verdad que en ocasiones el entusiasmo del escritor le lleva a algún exceso cuando alcanza las fronteras del conocimiento actual, como es poner la emergencia de la autoconsciencia humana (una opinión respetable, pero no sistematizada científicamente) en el mismo saco que la superconductividad; pero en general el tono es riguroso.

Ahora bien, tratar sobre la naturaleza de la luz, los conceptos de campos de fuerzas y de transiciones de fase, las teorías de la gravitación y la relatividad, la cosmología y los mitos de la creación del universo a lo largo de la historia, es intentar abarcar demasiado. Aunque la intención sea buena, el resultado final es que lo tratado no responde al título: sólo en los dos últimos capítulos, apenas la cuarta parte del libro, se aborda la cuestión planteada de manera sistemática. Para entonces poco se puede hacer ya; en un libro de divulgación las páginas se van acumulando con la misma rapidez que los avisos en las corridas de toros, y ha de rematarse la faena. Así, el tema que se enuncia al principio de la obra se despacha con excesiva rapidez. Da la impresión de que la nada no es sino el gancho del que se sirve el autor para elaborar un personal recorrido por la historia de la ciencia. Cierto, la narración es amena e interesante, pero queda la desazón de no haber entrado en materia —si es que la nada es materia.

Angel Garcimartín

EN EL PROXIMO NUMERO DE DICIEMBRE 2008

La gran implosión cósmica,

por Martin Bojowald

Nuestro universo quizá no empezó con una gran explosión, sino con una gran implosión, que desencadenó, por efectos cuánticos exóticos, una explosión.



KENN BROWN

Partículas bellas de materia y antimateria,

por Alberto Ruiz Jimeno

A la física de partículas le aguardan días de esplendor ahora que entra en funcionamiento en el CERN el acelerador más potente jamás construido. Mientras, el Tevatrón ha seguido comprobando la validez del modelo estándar y descubriendo nuevas partículas.



Código de barras biológico,

por Mark Y. Stoeckle y Paul D. N. Hebert

Las etiquetas de ADN, inspiradas en los códigos de barras comerciales, proporcionarían un medio rápido y barato para la identificación de especies.



En busca de la inteligencia,

por Carl Zimmer

La detección en nuestros genes de factores que configuren la inteligencia está resultando más escurridiza de lo esperado.

El nacimiento de un océano,

por Eitan Haddok

En uno de los rincones más calurosos e inhóspitos del planeta se está produciendo un acontecimiento excepcional: la formación de una cuenca oceánica. Un reportaje fotográfico nos ofrece la oportunidad de presenciar ese fenómeno geofísico.

